(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平11－167551

(43)公開日　平成11年(1999)６月22日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｆ　15/00	３１０	Ｇ０６Ｆ　15/00	３１０Ｄ
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７３Ｄ

審査請求　有　　請求項の数13　ＯＬ　（全 40 頁）

(21)出願番号　特願平9－332889

(22)出願日　平成９年(1997)12月３日

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号

(72)発明者　白木　宏明
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内

(72)発明者　釜坂　等
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内

(72)発明者　虎渡　昌史
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内

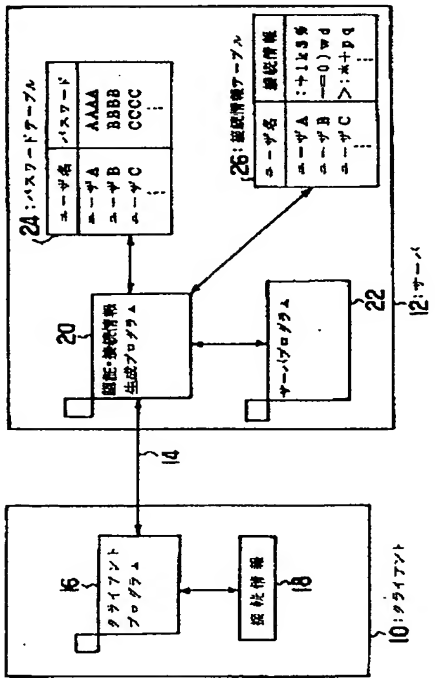
(74)代理人　弁理士　吉田　研二　（外２名）

(54)【発明の名称】　サーバ、サーバのアクセス制御方法および情報記録媒体

(57)【要約】

【課題】　クライアントサーバ間のアクセス制御において認証情報の漏洩の可能性を少なくする。

【解決手段】　コネクションレス環境にあるクライアント１０とサーバ１２とのアクセス制御において、パスワードテーブル２４によるユーザ認証に成功したクライアント１０にサーバ１２から接続情報を生成して送信するとともに、その接続情報をサーバ１２の接続情報テーブル２６で記憶しておく。そして、サーバ１２では、クライアント１０から要求信号と対応づけられた接続情報を受信した場合に、その接続情報と接続情報テーブル２６で記憶される接続情報とに基づいて、クライアント１０のユーザ認証を行う。そして、このユーザ認証に成功すれば、接続情報と対応づけられた要求信号に対応するサーバ情報をサーバプログラム２２から取得してクライアント１０に返信する。



1

【特許請求の範囲】

【請求項１】　クライアントから送信される要求信号に対応するサーバ情報を、そのクライアントに返信するサーバにおいて、

パスワードによるユーザ認証に成功したクライアントに接続情報を生成して送信する接続情報送信手段と、

前記接続情報送信手段によりクライアントに送信する接続情報を記憶する接続情報記憶手段と、

クライアントから要求信号と対応づけられた接続情報を受信した場合に、その接続情報と前記接続情報記憶手段に記憶される接続情報とに基づいて、クライアントのユーザ認証を行う認証手段と、

前記認証手段によりクライアントのユーザ認証に成功した場合に、その接続情報と対応づけられた要求信号に対応するサーバ情報をクライアントに返信するサーバ情報返信手段と、

を含むことを特徴とするサーバ。

【請求項２】　クライアントから同一の接続情報を所定回数以上受信した場合に、新たな接続情報を生成してクライアントに送信するとともに、その新たな接続情報を前記接続情報記憶手段に記憶する第１の接続情報更新手段をさらに含むことを特徴とする請求項１記載のサーバ。

【請求項３】　前記接続情報送信手段による接続情報の生成から所定時間が経過した場合に、新たな接続情報を生成してクライアントに送信するとともに、その新たな接続情報を前記接続情報記憶手段に記憶する第２の接続情報更新手段をさらに含むことを特徴とする請求項１又は２記載のサーバ。

【請求項４】　前回のアクセスの時点から所定時間が経過しても再び同じクライアントからのアクセスがない場合に、前記認証手段によるクライアントのユーザ認証を一旦中止する第１の認証中止手段をさらに含むことを特徴とする請求項１乃至３のいずれかに記載のサーバ。

【請求項５】　パスワードによるクライアントのユーザ認証の後、所定回数以上そのクライアントからのアクセスがあった場合に、前記認証手段によるクライアントのユーザ認証を一旦中止する第２の認証中止手段をさらに含むことを特徴とする請求項１乃至４のいずれかに記載のサーバ。

【請求項６】　パスワードによるクライアントのユーザ認証の後、所定時間が経過した場合に、前記認証手段によるクライアントのユーザ認証を一旦中止する第３の認証中止手段をさらに含むことを特徴とする請求項１乃至５のいずれかに記載のサーバ。

【請求項７】　クライアントから接続情報を無効化すべき旨の所定の要求信号を受信した場合に、前記認証手段によるクライアントのユーザ認証を中止する第４の認証中止手段をさらに含むことを特徴とする請求項１乃至６のいずれかに記載のサーバ。

2

【請求項８】　接続情報を用いた一定時間毎のクライアントからサーバへのアクセスを発生させるクライアントサーバ間アクセス発生手段をさらに含むことを特徴とする請求項１乃至７のいずれかに記載のサーバ。

【請求項９】　前記クライアントサーバ間アクセス発生手段は、クライアントに対し、接続情報を用いたサーバへのアクセスを一定時間毎に行うよう、クライアントを制御する実行モジュールを送信する実行モジュール送信手段を含むことを特徴とする請求項８記載のサーバ。

【請求項１０】　前記サーバ情報はハイパーテキスト情報であって、

前記クライアントサーバ間アクセス発生手段は、接続情報を用いたサーバへのアクセスを所定時間後に行うべき旨のタグ情報を前記サーバ情報に含めることを特徴とする請求項８記載のサーバ。

【請求項１１】　クライアントから暗号化されたパスワードが送信された場合に、該パスワードを復号化する復号化手段をさらに備えることを特徴とする請求項１乃至９のいずれかに記載のサーバ。

【請求項１２】　クライアントから送信される要求信号に対応するサーバ情報を、そのクライアントに返信するサーバのアクセス制御方法であって、

パスワードによるユーザ認証に成功したクライアントに接続情報を生成して送信する接続情報送信ステップと、

前記接続情報送信ステップでクライアントに送信する接続情報を記憶する接続情報記憶ステップと、

クライアントから要求信号と対応づけられた接続情報を受信した場合に、その接続情報と前記接続情報記憶ステップで記憶される接続情報とに基づいて、クライアントのユーザ認証を行う認証ステップと、

前記認証ステップでクライアントのユーザ認証に成功した場合に、その接続情報と対応づけられた要求信号に対応するサーバ情報をクライアントに返信するサーバ情報返信ステップと、

を含むことを特徴とするサーバのアクセス制御方法。

【請求項１３】　コンピュータを、クライアントから送信される要求信号に対応するサーバ情報を、そのクライアントに返信するサーバとして動作させるためのプログラムを記録した情報記録媒体であって、

パスワードによるユーザ認証に成功したクライアントに接続情報を生成して送信する接続情報送信ステップと、

前記接続情報送信ステップでクライアントに送信する接続情報を記憶する接続情報記憶ステップと、

クライアントから要求信号と対応づけられた接続情報を受信した場合に、その接続情報と前記接続情報記憶ステップで記憶される接続情報とに基づいて、クライアントのユーザ認証を行う認証ステップと、

前記認証ステップでクライアントのユーザ認証に成功した場合に、その接続情報と対応づけられた要求信号に対応するサーバ情報をクライアントに返信するサーバ情報

返信ステップと、
をコンピュータに実行させるためのプログラムを記録したことを特徴とする情報記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、サーバ、サーバのアクセス制御方法および情報記録媒体に関し、特にサーバのクライアントに対するアクセス制御技術に関する。

【０００２】

【従来の技術】クライアントからの要求信号に対してサーバが対応するサーバ情報をそのクライアントに返信するコネクションレス環境においては、クライアントサーバ間で通信接続が維持されない。したがって、クライアントプログラムがアクセス制御されているサーバ上の情報を獲得しようとすれば、既にユーザ認証に成功している場合であっても、クライアントがサーバに要求信号を送信する度にユーザ名やパスワードの入力による認証が必要とされる。このため、ユーザはサーバに要求信号を送信する場合、クライアントにてユーザ名とパスワードとを入力し、それらをサーバに送信しなくてはならず、操作が煩雑になるという問題があった。

【０００３】これに対して、クライアントのマシン上のメモリにユーザ名とパスワードとを記憶しておき、あるサーバに対するアクセスにおいてユーザ名とパスワードによるユーザ認証に一度成功すれば、その後の同じサーバへのアクセスではメモリ上のユーザ名とパスワードを毎回自動送信することにより、かかる問題を回避することも考えられる。

【０００４】

【発明が解決しようとする課題】しかしながら、クライアントサーバ間のアクセス制御においては、ユーザ名やパスワード等の認証情報が単純なテキストデータで送信されることも多く、上述のようにクライアントからサーバへのアクセスの度にパスワードを送信することは、盗聴の危険性を増し、ユーザへの成りすましによる不正アクセスを招きやすいという問題がある。

【０００５】一方、特開平４－１８２７６８号公報に係る機密保護方式においては、コネクションを確立する通信環境において、アクセスのたびに機密照会情報を変更している。すなわち、この方式においては、ホストコンピュータとのコネクション確立のために、固定のパスワード情報と毎回変わる機密照会情報とを対で用いることにより、クライアントのユーザ認証を行う。しかしながら、この技術においてもクライアントとホストコンピュータとの間で頻繁にパスワードの送受が行われるため、これらの情報の盗聴の危険性が高い。さらにクライアントに機密照会情報が保存されるため、そのクライアントからしかホストコンピュータにアクセスすることができないという問題がある。

【０００６】本発明は上記課題に鑑みてなされたものであって、その目的は、クライアントサーバ間のアクセス制御において認証情報の漏洩の可能性を少なくすることができるサーバ、サーバのアクセス制御方法およびそれを実現するプログラムを記録した情報記録媒体を提供することにある。

【０００７】

【課題を解決するための手段】上記課題を解決するために、第１の発明は、クライアントから送信される要求信号に対応するサーバ情報を、そのクライアントに返信するサーバにおいて、パスワードによるユーザ認証に成功したクライアントに接続情報を生成して送信する接続情報送信手段と、前記接続情報送信手段によりクライアントに送信する接続情報を記憶する接続情報記憶手段と、クライアントから要求信号と対応づけられた接続情報を受信した場合に、その接続情報と前記接続情報記憶手段に記憶される接続情報とに基づいて、クライアントのユーザ認証を行う認証手段と、前記認証手段によりクライアントのユーザ認証に成功した場合に、その接続情報と対応づけられた要求信号に対応するサーバ情報をクライアントに返信するサーバ情報返信手段と、を含むものである。

【０００８】第２の発明は、第１の発明において、クライアントから同一の接続情報を所定回数以上受信した場合に、新たな接続情報を生成してクライアントに送信するとともに、その新たな接続情報を前記接続情報記憶手段に記憶する第１の接続情報更新手段をさらに含むものである。

【０００９】第３の発明は、第１又は第２の発明において、前記接続情報送信手段による接続情報の生成から所定時間が経過した場合に、新たな接続情報を生成してクライアントに送信するとともに、その新たな接続情報を前記接続情報記憶手段に記憶する第２の接続情報更新手段をさらに含むものである。

【００１０】第４の発明は、第１乃至第３のいずれかの発明において、前回のアクセスの時点から所定時間が経過しても再び同じクライアントからのアクセスがない場合に、前記認証手段によるクライアントのユーザ認証を一旦中止する第１の認証中止手段をさらに含むものである。

【００１１】第５の発明は、第１乃至第４のいずれかの発明において、パスワードによるクライアントのユーザ認証の後、所定回数以上そのクライアントからのアクセスがあった場合に、前記認証手段によるクライアントのユーザ認証を一旦中止する第２の認証中止手段をさらに含むものである。

【００１２】第６の発明は、第１乃至第５のいずれかの発明において、パスワードによるクライアントのユーザ認証の後、所定時間が経過した場合に、前記認証手段によるクライアントのユーザ認証を一旦中止する第３の認証中止手段をさらに含むものである。

【００１３】第７の発明は、第１乃至第６のいずれかの発明において、クライアントから接続情報を無効化すべき旨の所定の要求信号を受信した場合に、前記認証手段によるクライアントのユーザ認証を中止する第４の認証中止手段をさらに含むものである。

【００１４】第８の発明は、第１乃至第７のいずれかの発明において、接続情報を用いた一定時間毎のクライアントからサーバへのアクセスを発生させるクライアントサーバ間アクセス発生手段をさらに含むものである。

【００１５】第９の発明は、第８の発明において、前記クライアントサーバ間アクセス発生手段は、クライアントに対し、接続情報を用いたサーバへのアクセスを一定時間毎に行うよう、クライアントを制御する実行モジュールを送信する実行モジュール送信手段を含むものである。

【００１６】第１０の発明は、第８の発明において、前記サーバ情報はハイパーテキスト情報であって、前記クライアントサーバ間アクセス発生手段は、接続情報を用いたサーバへのアクセスを所定時間後に行うべき旨のタグ情報を前記サーバ情報に含めるものである。

【００１７】第１１の発明は、第１乃至第９のいずれかの発明において、クライアントから暗号化されたパスワードが送信された場合に、該パスワードを復号化する復号化手段をさらに備えるものである。

【００１８】第１２の発明は、クライアントから送信される要求信号に対応するサーバ情報を、そのクライアントに返信するサーバのアクセス制御方法であって、パスワードによるユーザ認証に成功したクライアントに接続情報を生成して送信する接続情報送信ステップと、前記接続情報送信ステップでクライアントに送信する接続情報を記憶する接続情報記憶ステップと、クライアントから要求信号と対応づけられた接続情報を受信した場合に、その接続情報と前記接続情報記憶ステップで記憶される接続情報とに基づいて、クライアントのユーザ認証を行う認証ステップと、前記認証ステップでクライアントのユーザ認証に成功した場合に、その接続情報と対応づけられた要求信号に対応するサーバ情報をクライアントに返信するサーバ情報返信ステップと、を含むものである。

【００１９】第１３の発明は、コンピュータを、クライアントから送信される要求信号に対応するサーバ情報を、そのクライアントに返信するサーバとして動作させるためのプログラムを記録した情報記録媒体であって、パスワードによるユーザ認証に成功したクライアントに接続情報を生成して送信する接続情報送信ステップと、前記接続情報送信ステップでクライアントに送信する接続情報を記憶する接続情報記憶ステップと、クライアントから要求信号と対応づけられた接続情報を受信した場合に、その接続情報と前記接続情報記憶ステップで記憶される接続情報とに基づいて、クライアントのユーザ認証を行う認証ステップと、前記認証ステップでクライアントのユーザ認証に成功した場合に、その接続情報と対応づけられた要求信号に対応するサーバ情報をクライアントに返信するサーバ情報返信ステップと、をコンピュータに実行させるためのプログラムを記録したものである。

【００２０】

【発明の実施の形態】以下、本発明の実施の形態について図面に基づき詳細に説明する。

【００２１】実施の形態１．図１は、本発明の実施の形態１に係る通信システムを示す機能ブロック図である。以下では、この通信システムの開示を通じて、本発明に係るサーバ、クライアント、サーバのアクセス制御方法およびそれを実現するためのプログラムを記録した情報記録媒体の実施形態の一つについて明らかにする。

【００２２】同図に示すように、本通信システムは、クライアント１０とサーバ１２とがインターネット等の通信手段１４により相互に通信可能に接続されてなる。そして、本通信システムにおいてクライアント１０とサーバ１２はコネクションレス環境にて通信接続されており、クライアント１０はサーバ１２に対してサーバ情報を要求する旨の要求信号を送信する。一方、サーバ１２はクライアント１０から受信する要求信号に対応するサーバ情報をそのクライアント１０に返信する。かかる構成はWWW（World Wide Web）システムなどで一般的であり、この場合、上記要求信号はＵＲＬ（Uniform Resource Locator）に相当し、上記サーバ情報はハイパーテキスト情報に相当する。

【００２３】クライアント１０は、ＰＣ等の情報処理装置により構成され、主記憶装置にロードされＣＰＵにより実行されるクライアントプログラム１６を含んでいる。そして、特にメモリ等の記憶手段１８には接続情報が記憶されている。かかるクライアントプログラム１６は、通信手段１４を介してサーバ１２に要求信号を送信するとともに、その要求信号に対してサーバ１２からサーバ情報を受信すれば、図示しない表示装置によりそのサーバ情報に基づくディスプレイ表示を行う。また、クライアントプログラム１６は記憶手段１８に接続情報が記憶されている場合にはその接続情報を要求信号とともにサーバ１２に送信する。

【００２４】サーバ１２は、クライアント１０と同様、ＰＣ等の情報処理装置により構成されており、主記憶装置にロードされＣＰＵにより実行される、認証・接続情報生成プログラム２０と、サーバプログラム２２と、を含んでいる。そして、特にその外部記憶装置にはパスワードテーブル２４と接続情報テーブル２６とが記憶されている。

【００２５】認証・接続情報生成プログラム２０は、まず、クライアントプログラム１６からユーザ名やパスワードが送信された場合に、その情報とパスワードテーブ

ル２４とに基づいてクライアント１０のユーザ認証を行う。そして、クライアント１０のユーザ認証に成功した場合には、そのクライアント１０に対する接続情報を生成してクライアント１０に送信するとともに、該情報をユーザ名と対応づけて接続情報テーブル２６に記憶する。

【００２６】また、認証・接続情報生成プログラム２０は、クライアントプログラム１６から要求信号とともに接続情報が送信された場合に、その接続情報と接続情報テーブル２６とに基づいてクライアント１０のユーザ認証を行う。そして、クライアント１０のユーザ認証に成功した場合にはサーバプログラム２２に対してクライアント１０が要求するサーバ情報の送信をサーバプログラム２２に要求し、サーバプログラム２２から受信するサーバ情報をクライアント１０に送信する。

【００２７】ここで、サーバプログラム２２は、要求信号を受信した場合に対応するサーバ情報を返信するプログラムである。また、パスワードテーブル２４には、サーバ１２がアクセスされることを予定しているユーザのユーザ名（ＩＤ）と、そのユーザに与えられたパスワードと、が対応づけられて記憶されている。さらに、接続情報テーブル２６は、認証・接続情報生成プログラム２０により生成される接続情報が記憶されるテーブルであり、サーバ１２にアクセスしたクライアント１０のユーザ名と、そのユーザ名に対して生成された接続情報と、が対応づけられて記憶されている。

【００２８】なお、以上の通信システムに含まれるサーバ１２においては、認証・接続情報生成プログラム２０は、パスワードによるユーザ認証に成功したクライアント１０に接続情報を生成して送信する接続情報送信手段として機能する。また、接続情報テーブル２６は、接続情報送信手段によりクライアント１０に送信する接続情報を記憶する接続情報記憶手段として機能する。さらに、認証・接続情報生成プログラム２０は、クライアント１０から要求信号と対応づけられた接続情報を受信した場合に、その接続情報と接続情報記憶手段に記憶される接続情報とに基づいて、クライアント１０のユーザ認証を行う認証手段として機能するとともに、認証手段によりクライアント１０のユーザ認証に成功した場合に、その接続情報と対応づけられた要求信号に対応するサーバ情報をクライアント１０に送信するサーバ情報返信手段として機能する。

【００２９】以下、かかる構成を有する本通信システムの動作について図２および図３に示すフロー図に基づいて説明する。

【００３０】図２に示すように、まず、サーバ１２では、認証・接続情報生成プログラム２０がクライアント１０からの要求信号を受信する（Ｓ１０１）。そして、その受信した要求信号に接続情報が含まれているか否かを判断し（Ｓ１０２）、接続情報が含まれていなければクライアント１０に対してユーザ名とパスワードを要求する（Ｓ１０３）。これに対してクライアント１０からユーザ名とパスワードを受信すれば（Ｓ１０４）、次に認証・接続情報生成プログラム２０は、その受信したユーザ名およびパスワードとパスワードテーブル２４とに基づいて、クライアント１０のユーザ認証を行う。そして、パスワードテーブル２４によるクライアント１０のユーザ認証に失敗すれば（Ｓ１０５）、クライアント１０とサーバ１２との間の通信処理を終了する。

【００３１】また、Ｓ１０５において認証・接続情報生成プログラム２０がパスワードテーブル２４によるクライアント１０のユーザ認証に成功すれば、接続情報を生成し（Ｓ１０６）、その接続情報を接続情報テーブル２６にユーザ名とともに追加記録する（Ｓ１０７）。この接続情報は数字、記号、文字のランダムな組み合わせにより、暗号化して生成される。次に、認証・接続情報生成プログラム２０は、サーバプログラム２２にユーザ名等のユーザ情報を送信するとともに（Ｓ１０８）、サーバ情報を獲得するための要求信号を送信する（Ｓ１０９）。サーバプログラム２２に送信されるユーザ情報は当該サーバプログラム２２にて必要であれば使用することができる。そして、認証・接続情報生成プログラム２０は、Ｓ１０６で生成した接続情報をクライアント１０に送信するとともに（Ｓ１１０）、サーバプログラム２２から受信したサーバ情報をクライアント１０に送信する（Ｓ１１１）。

【００３２】一方、Ｓ１０２において認証・接続情報生成プログラム２０がクライアント１０から受信する要求信号に接続情報が含まれていると判断した場合には、次に該認証・接続情報生成プログラム２０はその接続情報が接続情報テーブル２６に既に記録されているものと同一であるかを調べることによりクライアント１０のユーザ認証を行う（Ｓ１１２）。そして、クライアント１０のユーザ認証に成功すれば（Ｓ１１３）、Ｓ１０８に処理を移し、クライアント１０に対してサーバ情報を返信するための処理を行う。また、Ｓ１１３においてクライアント１０のユーザ認証に失敗すればクライアント１０とサーバ１２との間の通信を終了する。

【００３３】以上説明した実施の形態によれば、クライアント１０とサーバ１２との間でパスワードのやり取りが行われる回数を少なくすることができるため、パスワードの漏洩による不正アクセスを防止することができる。また、接続情報を頻繁に変更して、いわば動的なパスワードとして機能させることができ、こうすれば接続情報事態の漏洩をも防止することができ、さらに確実に不正アクセスを防止することができる。

【００３４】実施の形態２．図４は、本発明の実施の形態２に係る通信システムを示す機能ブロック図である。同図に示す通信システムは、パスワードテーブル２４ａと接続情報テーブル２６ａの内容と認証・接続情報生成

プログラム２０ａの処理と、にその特徴を有するものである。そして、クライアント１０およびその内部構成とサーバ１２ａのサーバプログラム２２は、実施の形態１に係る通信システムと同様であるので、ここでは同一符号を付して説明を省略する。

【００３５】まず、本実施の形態に係る通信システムのパスワードテーブル２４ａには、ユーザ名とパスワードとに対応づけて、各ユーザの接続情報変更回数が記憶されている。この接続情報変更回数は接続情報テーブル２６ａに記憶されている接続情報の更新条件を決める設定値であり、図示しない入力手段によりクライアント１０又はサーバ１２のユーザにより予め設定入力される。

【００３６】また、本実施の形態に係る通信システムの接続情報テーブル２６ａには、ユーザ名と接続情報に対応づけて、各ユーザのアクセス回数が記憶されている。このアクセス回数は接続情報が生成されて接続情報テーブル２６ａに格納されてから後の、そのクライアント１０のアクセス回数を表す。

【００３７】一方、本通信システムの認証・接続情報生成プログラム２０ａは、クライアント１０のアクセスがある毎に接続情報テーブル２６のアクセス回数の欄をインクリメントして更新する。そして、そのアクセス回数がパスワードテーブル２４ａに記憶されている接続情報変更回数の値に達すれば、新たな接続情報を生成してクライアント１０に送信するとともに、接続情報テーブル２６ａに既に記録されている接続情報の値を新たなものに更新する。また、このときアクセス回数の値を０にリセットする。

【００３８】すなわち、本実施の形態においては、認証・接続情報生成プログラム２０ａが、クライアントから同一の接続情報を所定回数以上受信した場合に、新たな接続情報を生成してクライアント１０に送信するとともに、その新たな接続情報を接続情報テーブル２６ａに記憶する第１の接続情報更新手段としても機能する。

【００３９】以下、かかる構成を有する本通信システムの動作について図５および図６に示すフロー図に基づいて説明する。ここで、図５に示すフロー図は、図２に示すフロー図においてＳ１０７とＳ１０８との間に接続情報テーブル２６ａのアクセス回数を０にリセットする処理フローＳ２００を追加したものであるから、その他の処理については図２と同一符号を付し、ここでは簡単な説明に留める。

【００４０】まず、図５に示すフロー図において、認証・接続情報生成プログラム２０ａがクライアント１０から要求信号を受信し（Ｓ１０１）、その要求信号に接続情報が含まれている場合には（Ｓ１０２）、図６に示すように、その接続情報と接続情報テーブル２６とに基づいてクライアント１０のユーザ認証を行う（Ｓ２０１）。そして、接続情報を用いたクライアント１０のユーザ認証に失敗すれば、クライアント１０とサーバ１２との間の通信を終了する。

【００４１】一方、接続情報を用いたクライアント１０のユーザ認証に成功すれば、認証・接続情報生成プログラム２０は、次に接続情報テーブル２６ａに記憶されているアクセス回数の値をインクリメントして接続情報テーブル２６ａのアクセス回数の値ｎを更新する（Ｓ２０２）。さらに認証・接続情報生成プログラム２０は、パスワードテーブル２４ａから接続情報変更回数の値Ｋを読み出し（Ｓ２０３）、その値とアクセス回数の値とを比較する（Ｓ２０４）。そして、アクセス回数の値ｎが接続情報変更回数の値Ｋよりも小さな値であれば、Ｓ１０８（図５）に処理を移して通常通りサーバプログラム２２へのアクセス処理を行う（Ｓ１０８）。一方、アクセス回数の値ｎが接続情報変更回数の値Ｋ以上であれば、認証・接続情報生成プログラム２０は新たな接続情報を生成し（Ｓ２０５）、それを接続情報テーブル２６に格納して接続情報を更新する（Ｓ２０６）。さらに、認証・接続情報生成プログラム２０は接続情報テーブル２６のアクセス回数の値ｎを０にリセットする（Ｓ２００，図５）。その後、通常通りサーバプログラム２２へのアクセス処理を行う（Ｓ１０８）。この際、Ｓ１１０においてクライアント１０に送信される接続情報はＳ２０５において新たに生成されたものである。クライアントプログラム１６は、この新たな接続情報をサーバ１２から受信し、記憶手段１８に既に記憶されている古い接続情報を更新する。

【００４２】以上説明した実施の形態によれば、アクセス回数が一定回数以上になったときに接続情報が更新される。これにより、接続情報が盗聴される可能性を少なくすることができるとともに、もしも接続情報が盗聴された場合にも、その接続情報を用いた成りすましによる不正アクセスを制限することができる。

【００４３】実施の形態３．図７は、本発明の実施の形態３に係る通信システムを示す機能ブロック図である。同図に示す通信システムは、実施の形態１又は２に係る通信システムに比して、パスワードテーブル２４ｂと接続情報テーブル２６ｂの内容と認証・接続情報生成プログラム２０ｂの処理と、にその特徴を有するものである。そして、クライアント１０の構成とサーバ１２ｂのサーバプログラム２２は、実施の形態１又は２に係る通信システムと同様であるので、ここでは同一符号を付して説明を省略する。

【００４４】まず、本実施の形態に係る通信システムのパスワードテーブル２４ｂには、ユーザ名とパスワードとに対応づけて、各ユーザの接続情報変更経過時間が記憶されている。この接続情報変更経過時間は接続情報テーブル２６ｂに記憶されている接続情報の更新条件を決める設定値であり、図示しない入力手段によりクライアント１０又はサーバ１２ｂのユーザにより予め設定入力される。

【００４５】また、本実施の形態に係る通信システムの接続情報テーブル２６ｂには、ユーザ名と接続情報に対応づけて、各ユーザの接続情報生成時刻が記憶されている。この接続情報生成時刻は接続情報が生成された時刻を表す。

【００４６】一方、本通信システムの認証・接続情報生成プログラム２０ｂは、クライアント１０のアクセスがある毎に接続情報テーブル２６ｂの接続情報生成時刻からの経過時間を計算する。そして、その計算した経過時間がパスワードテーブル２４ｂに記憶されている接続情報変更経過時間の値に達すれば、新たな接続情報を生成してクライアント１０に送信するとともに、接続情報テーブル２６ｂに既に記録されている接続情報の値を新たなものに更新する。また、このとき接続情報生成時刻をその時点の時刻に再設定して更新する。

【００４７】すなわち、本実施の形態においては、認証・接続情報生成プログラム２０ｂが、接続情報の生成から所定時間が経過した場合に、新たな接続情報を生成してクライアント１０に送信するとともに、その新たな接続情報を接続情報テーブル２６ｂに記憶する第２の接続情報更新手段としても機能する。

【００４８】以下、かかる構成を有する本通信システムの動作について図８および図９に示すフロー図に基づいて説明する。ここで、図８に示すフロー図は、図２に示すフロー図においてＳ１０７とＳ１０８との間に接続情報テーブル２６ｂの接続情報生成時刻を更新する処理フローＳ３００を追加したものであるから、その他の処理については図２と同一符号を付し、ここでは簡単な説明に留める。

【００４９】まず、図８に示すフロー図において、認証・接続情報生成プログラム２０ｂがクライアント１０から要求信号を受信し（Ｓ１０１）、その要求信号に接続情報が含まれている場合には（Ｓ１０２）、図９に示すように、その接続情報と接続情報テーブル２６ｂとに基づいてクライアント１０のユーザ認証を行う（Ｓ３０１）。そして、接続情報を用いたクライアント１０のユーザ認証に失敗すれば、クライアント１０とサーバ１２ｂとの間の通信を終了する。

【００５０】一方、接続情報を用いたクライアント１０のユーザ認証に成功すれば、認証・接続情報生成プログラム２０ｂは、次に接続情報テーブル２６ｂに記憶されている接続情報生成時刻を図示しない内部クロックから出力された現在時刻から減算し、接続情報を生成した時点から現在までの経過時間ｔを導出する（Ｓ３０２）。さらに認証・接続情報生成プログラム２０は、パスワードテーブル２４ａから接続情報変更経過時間Ｔを読み出し（Ｓ３０３）、その値とＳ３０２で導出した経過時間ｔの値とを比較する（Ｓ３０４）。

【００５１】そして、経過時間ｔが接続情報変更経過時間Ｔよりも小さな値であれば、Ｓ１０８（図８）に処理を移して通常通りサーバプログラム２２へのアクセス処理を行う（Ｓ１０８）。一方、経過時間ｔが接続情報変更経過時間Ｔ以上であれば、認証・接続情報生成プログラム２０ｂは新たな接続情報を生成し（Ｓ３０５）、それを接続情報テーブル２６ｂに格納して接続情報を更新する（Ｓ３０６）。さらに、認証・接続情報生成プログラム２０ｂは接続情報テーブル２６ｂの接続情報生成時刻の値を図示しない内部クロックから出力される現在時刻に再設定する（Ｓ３００，図８）。その後、通常通りサーバプログラム２２へのアクセス処理を行う（Ｓ１０８）。この際、Ｓ１１１においてクライアント１０に送信される接続情報はＳ３０５において新たに生成されたものである。クライアントプログラム１６は、この新たな接続情報をサーバ１２ｂから受信し、記憶手段１８に既に記憶されている古い接続情報を更新する。

【００５２】以上説明した本実施の形態によれば、接続情報を生成した時刻から一定時間が経過した場合に接続情報が更新される。すなわち、同一の接続情報によりサーバでユーザ認証を受けることができる期間が一定期間に制限される。これにより、接続情報が盗聴される可能性を少なくすることができるとともに、もしも接続情報が盗聴された場合にも、その接続情報を用いた成りすましによる不正アクセスを制限することができる。

【００５３】実施の形態４．図１０は、本発明の実施の形態４に係る通信システムを示す機能ブロック図である。同図に示す通信システムは、上記実施の形態２に係る通信システムの技術と上記実施の形態３に係る通信システムの技術との組み合わせに係るものであり、パスワードテーブル２４ｃと接続情報テーブル２６ｃの内容と認証・接続情報生成プログラム２０ｃの処理と、にその特徴を有するものである。そして、クライアント１０およびその内部構成とサーバ１２ｃのサーバプログラム２２は、実施の形態１に係る通信システムと同様であるので、ここでは同一符号を付して説明を省略する。

【００５４】まず、本実施の形態に係る通信システムのパスワードテーブル２４ｃには、ユーザ名とパスワードとに対応づけて、各ユーザの接続情報変更回数と接続情報変更経過時刻とが記憶されている。接続情報変更回数は、上記実施の形態２と同様、接続情報テーブル２６ｃに記憶されている接続情報の更新条件を決める設定値であり、図示しない入力手段によりクライアント１０又はサーバ１２ｃのユーザにより予め設定入力される。また、接続情報変更経過時間は、上記実施の形態３と同様、接続情報テーブル２６ｃに記憶されている接続情報の更新条件を決める設定値であり、図示しない入力手段によりクライアント１０又はサーバ１２ｃのユーザにより予め設定入力される。

【００５５】また、本実施の形態に係る通信システムの接続情報テーブル２６ｃには、ユーザ名と接続情報に対応づけて、各ユーザのアクセス回数と接続情報生成時刻

とが記憶されている。アクセス回数は、上記実施の形態２と同様、接続情報が生成されて接続情報テーブル２６ｃに格納されてから後の、そのクライアント１０のアクセス回数を表す。また、接続情報生成時刻は、上記実施の形態３と同様、接続情報が生成された時刻を表す。

【００５６】一方、本通信システムの認証・接続情報生成プログラム２０ｃは、クライアント１０のアクセスがある毎に接続情報テーブル２６ｃのアクセス回数の欄をインクリメントして更新する。そして、そのアクセス回数がパスワードテーブル２４ｃに記憶されている接続情報変更回数の値に達すれば、新たな接続情報を生成してクライアント１０に送信するとともに、接続情報テーブル２６ｃに既に記録されている接続情報の値を新たなものに更新する。また、このときアクセス回数の値を０にリセットする。さらに、認証・接続情報生成プログラム２０ｃは、クライアント１０のアクセスがある毎に接続情報テーブル２６ｃの接続情報生成時刻からの経過時間を計算する。そして、その計算した経過時間がパスワードテーブル２４ｃに記憶されている接続情報変更経過時間の値に達すれば、新たな接続情報を生成してクライアント１０に送信するとともに、接続情報テーブル２６ｃに既に記録されている接続情報の値を新たなものに更新する。また、このとき接続情報生成時刻をその時点の時刻に再設定して更新する。

【００５７】以下、かかる構成を有する本通信システムの動作について図１１および図１２に示すフロー図に基づいて説明する。ここで、図１１に示すフロー図は、図２に示すフロー図においてＳ１０７とＳ１０８との間に接続情報テーブル２６ｃのアクセス回数を０にリセットする処理フローＳ４００と接続情報テーブル２６ｃの接続情報生成時刻を更新する処理フローＳ４０１とを追加したものであるから、その他の処理については図２と同一符号を付し、ここでは簡単な説明に留める。

【００５８】まず、図５に示すフロー図において、認証・接続情報生成プログラム２０ｃがクライアント１０から要求信号を受信し（Ｓ１０１）、その要求信号に接続情報が含まれている場合には（Ｓ１０２）、図１２に示すように、その接続情報と接続情報テーブル２６ｃとに基づいてクライアント１０のユーザ認証を行う（Ｓ４０２）。そして、接続情報を用いたクライアント１０のユーザ認証に失敗すれば、クライアント１０とサーバ１２ｃとの間の通信を終了する。

【００５９】一方、接続情報を用いたクライアント１０のユーザ認証に成功すれば、認証・接続情報生成プログラム２０ｃは、次に接続情報テーブル２６ｃに記憶されているアクセス回数の値をインクリメントして接続情報テーブル２６ｃのアクセス回数の値ｎを更新する（Ｓ４０３）。さらに認証・接続情報生成プログラム２０ｃは、パスワードテーブル２４ｃから接続情報変更回数の値Ｋを読み出し（Ｓ４０４）、その値とアクセス回数の値とを比較する（Ｓ４０５）。

【００６０】そして、アクセス回数の値ｎが接続情報変更回数の値Ｋ以上の値であれば、認証・接続情報生成プログラム２０ｃは新たな接続情報を生成し（Ｓ４０９）、それを接続情報テーブル２６ｃに格納して接続情報を更新する（Ｓ４１０）。さらに、認証・接続情報生成プログラム２０ｃは接続情報テーブル２６ｃのアクセス回数の値ｎを０にリセットするとともに（Ｓ４００）、接続情報テーブル２６の接続情報生成時刻の値を図示しない内部クロックから出力される現在時刻に再設定する（Ｓ４０１）。その後、通常通りサーバプログラム２２へのアクセス処理を行う（Ｓ１０８）。この際、Ｓ１１１においてクライアント１０に送信される接続情報はＳ４０９において新たに生成されたものである。クライアントプログラム１６は、この新たな接続情報をサーバ１２ｂから受信し、記憶手段１８に既に記憶されている古い接続情報を更新する。

【００６１】一方、Ｓ４０５で、アクセス回数の値ｎが接続情報変更回数の値Ｋよりも小さな値であると判断されれば、次に、認証・接続情報生成プログラム２０ｃは、接続情報テーブル２６ｃに記憶されている接続情報生成時刻を図示しない内部クロックから出力された現在時刻から減算し、接続情報を生成した時点から現在までの経過時間ｔを導出する（Ｓ４０６）。さらに認証・接続情報生成プログラム２０ｃは、パスワードテーブル２４ｃから接続情報変更経過時間Ｔを読み出し（Ｓ４０７）、その値とＳ４０６で導出した経過時間ｔの値とを比較する（Ｓ４０８）。

【００６２】そして、経過時間ｔが接続情報変更経過時間Ｔよりも小さな値であれば、Ｓ１０８に処理を移して通常通りサーバプログラム２２へのアクセス処理を行う。一方、経過時間ｔが接続情報変更経過時間Ｔ以上であれば、認証・接続情報生成プログラム２０ｃは新たな接続情報を生成し（Ｓ４０９）、それを接続情報テーブル２６ｃに格納して接続情報を更新する（Ｓ４１０）。そして、認証・接続情報生成プログラム２０は接続情報テーブル２６のアクセス回数の値ｎを０にリセットするとともに（Ｓ４００）、接続情報テーブル２６の接続情報生成時刻の値を図示しない内部クロックから出力される現在時刻に再設定する（Ｓ４０１）。その後、通常通りサーバプログラム２２へのアクセス処理を行う（Ｓ１０８）。

【００６３】以上説明した本実施の形態によれば、接続情報を生成した時刻から一定時間が経過した場合、或いは接続情報を生成してから同一の接続情報によるアクセスが所定回数以上ある場合に、その接続情報が更新される。すなわち、同一の接続情報によりサーバでユーザ認証を受けることができる回数および期間が一定範囲に制限される。これにより、接続情報が盗聴される可能性を少なくすることができるとともに、もしも接続情報が盗

聴された場合にも、その接続情報を用いた成りすましによる不正アクセスを制限することができる。

【００６４】なお、上記説明においては、アクセス回数ｎが接続情報変更回数Ｋ以上である場合又は経過時間ｔが接続情報変更経過時間Ｔ以上である場合のいずれの場合にも接続情報を更新したが、アクセス回数ｎが接続情報変更回数Ｋ以上である場合であり、且つ経過時間ｔが接続情報変更経過時間Ｔ以上である場合にのみ接続情報を更新するようにしてもよい。

【００６５】実施の形態５．図１３は、本発明の実施の形態５に係る通信システムを示す機能ブロック図である。同図に示す通信システムは、上記各実施の形態に係る通信システムに比して、パスワードテーブル２４ｄと接続情報テーブル２６ｄの内容と認証・接続情報生成プログラム２０ｄの処理と、にその特徴を有するものである。そして、クライアント１０の構成とサーバ１２ｄのサーバプログラム２２は、上記各実施の形態に係る通信システムと同様であるので、ここでは同一符号を付して説明を省略する。

【００６６】まず、本実施の形態に係る通信システムのパスワードテーブル２４ｄには、ユーザ名とパスワードとに対応づけて、各ユーザのタイムアウト時間が記憶されている。このタイムアウト時間は接続情報テーブル２６ｄに記憶されている接続情報を削除する条件を決める設定値であり、図示しない入力手段によりクライアント１０又はサーバ１２ｄのユーザにより予め設定入力される。

【００６７】また、本実施の形態に係る通信システムの接続情報テーブル２６ｄには、ユーザ名と接続情報に対応づけて、各ユーザの前回アクセス時刻が記憶されている。この前回アクセス時刻は前回クライアント１０がサーバ１２ｄにアクセスした時刻を表す。

【００６８】一方、本通信システムの認証・接続情報生成プログラム２０ｄは、クライアント１０のアクセスがある毎に接続情報テーブル２６ｄの前回アクセス時刻からの経過時間を計算する。そして、その計算した経過時間がパスワードテーブル２４ｄに記憶されているタイムアウト時間の値に達すれば、接続情報テーブル２６ｄからそのユーザの接続情報を抹消し、再びクライアント１０に対してユーザ名とパスワードの送信を要求する。一方、その計算した経過時間がパスワードテーブル２４ｄに記憶されているタイムアウト時間に達していなければ、新たな接続情報を生成してクライアント１０に送信するとともに、接続情報テーブル２６ｄに既に記録されている接続情報の値を新たなものに更新する。また、このとき前回アクセス時刻をその時点の時刻に再設定して更新する。

【００６９】すなわち、本実施の形態においては、認証・接続情報生成プログラム２０ｄが、前回のアクセスの時点から所定時間が経過しても再び同じクライアントからのアクセスがない場合に、認証・接続情報生成プログラム２０ｄ（認証手段）によるクライアント１０のユーザ認証を一旦中止する第１の認証中止手段としても機能する。

【００７０】以下、かかる構成を有する本通信システムの動作について図１４および図１５に示すフロー図に基づいて説明する。ここで、図１４に示すフロー図は、図２に示すフロー図においてＳ１０７とＳ１０８との間に接続情報テーブル２６ｄの前回アクセス時刻を更新する処理フローＳ５００を追加したものであるから、その他の処理については図２と同一符号を付し、ここでは簡単な説明に留める。

【００７１】まず、図１４に示すフロー図において、認証・接続情報生成プログラム２０ｄがクライアント１０から要求信号を受信し（Ｓ１０１）、その要求信号に接続情報が含まれている場合には（Ｓ１０２）、図１５に示すように、その接続情報と接続情報テーブル２６ｄとに基づいてクライアント１０のユーザ認証を行う（Ｓ５０１）。そして、接続情報を用いたクライアント１０のユーザ認証に失敗すれば、クライアント１０とサーバ１２ｄとの間の通信を終了する。

【００７２】一方、接続情報を用いたクライアント１０のユーザ認証に成功すれば、認証・接続情報生成プログラム２０ｄは、次に接続情報テーブル２６ｄに記憶されている前回アクセス時刻を図示しない内部クロックから出力された現在時刻から減算し、当該クライアント１０が前回サーバ１２にアクセスした時刻から現在までの経過時間ｔを導出する（Ｓ５０２）。さらに認証・接続情報生成プログラム２０ｄは、パスワードテーブル２４ｄからタイムアウト時間Ｔを読み出し（Ｓ５０３）、その値とＳ５０２で導出した経過時間ｔの値とを比較する（Ｓ５０４）。

【００７３】そして、経過時間ｔがタイムアウト時間Ｔよりも小さな値であれば、認証・接続情報生成プログラム２０ｄは新たな接続情報を生成し（Ｓ５０５）、それを接続情報テーブル２６ｄに格納して接続情報を更新する（Ｓ５０６）。さらに、認証・接続情報生成プログラム２０ｄは接続情報テーブル２６ｄの前回アクセス時刻の値を図示しない内部クロックから出力される現在時刻に再設定する（Ｓ５００）。その後、通常通りサーバプログラム２２へのアクセス処理を行う（Ｓ１０８）。この際、Ｓ１１１においてクライアント１０に送信される接続情報はＳ５０５において新たに生成されたものである。クライアントプログラム１６は、この新たな接続情報をサーバ１２ｄから受信し、記憶手段１８に既に記憶されている古い接続情報を更新する。

【００７４】一方、経過時間ｔがタイムアウト時間Ｔ以上の値であれば、認証・接続情報生成プログラム２０ｄは接続情報テーブル２６ｄからそのクライアント１０の接続情報を抹消する（Ｓ５０７）。そうして、再びクラ

イアント１０に対してユーザ名とパスワードの送信を要求する（Ｓ１０３）。

【００７５】以上説明した本実施の形態によれば、クライアント１０からのアクセスの間隔が一定時間を超えた場合にその時点で登録している接続情報が接続情報テーブル２６ｄから削除される。すなわち、クライアント１０はサーバ１２ｄに対して一定時間以内で順次アクセスをしなければ接続情報が無効となり、再びユーザ名とパスワードによるユーザ認証が必要となる。こうして、本実施の形態によれば、接続情報が盗聴を防止することができ、この結果、成りすましによる不正アクセスを防止することができる。

【００７６】また、図１５のＳ５０４～Ｓ５０６で明らかなように、クライアント１０からサーバ１２ｄへのアクセスの度に接続情報が更新されるため、接続情報の盗聴の可能性を少なくすることができ、また、成りすましによる不正アクセスを防止することができる。

【００７７】実施の形態６．図１６は、本発明の実施の形態６に係る通信システムを示す機能ブロック図である。同図に示す通信システムは、上記各実施の形態に係る通信システムに比して、パスワードテーブル２４ｅと接続情報テーブル２６ｅの内容と認証・接続情報生成プログラム２０ｅの処理と、にその特徴を有するものである。そして、クライアント１０の構成とサーバ１２ｅのサーバプログラム２２は、上記各実施の形態に係る通信システムと同様であるので、ここでは同一符号を付して説明を省略する。

【００７８】まず、本実施の形態に係る通信システムのパスワードテーブル２４ｅには、ユーザ名とパスワードとに対応づけて、各ユーザの接続情報削除回数が記憶されている。この接続情報削除回数は接続情報テーブル２６ｅに記憶されている接続情報を削除する条件を決める設定値であり、図示しない入力手段によりクライアント１０又はサーバ１２ｅのユーザにより予め設定入力される。

【００７９】また、本実施の形態に係る通信システムの接続情報テーブル２６ｅには、ユーザ名と接続情報に対応づけて、実施例２に係る通信システムと同様、各ユーザのアクセス回数が記憶されている。このアクセス回数は新たな接続情報が生成されて接続情報テーブル２６ｅに格納されてから後の、そのクライアント１０のアクセス回数を表す。

【００８０】一方、本通信システムの認証・接続情報生成プログラム２０ｅは、クライアント１０のアクセスがある毎に接続情報テーブル２６ｅのアクセス回数の値をインクリメントして更新する。そして、そのアクセス回数がパスワードテーブル２４ｅに記憶されている接続情報削除回数の値に達すれば、接続情報テーブル２６ｅからそのユーザの接続情報を抹消し、再びクライアント１０に対してユーザ名とパスワードの送信を要求する。一方、アクセス回数がパスワードテーブル２４ｅに記憶されている接続情報削除回数に達していなければ、新たな接続情報を生成してクライアント１０に送信するとともに、接続情報テーブル２６ｅに既に記録されている接続情報の値を新たなものに更新する。

【００８１】本実施の形態においては、認証・接続情報生成プログラム２０ｅが、パスワードによるクライアント１０のユーザ認証の後、所定回数以上そのクライアントからのアクセスがあった場合に、認証・接続情報生成プログラム２０ｅ（認証手段）によるクライアント１０のユーザ認証を一旦中止する第２の認証中止手段としても機能する。

【００８２】以下、かかる構成を有する本通信システムの動作について図１７および図１８に示すフロー図に基づいて説明する。ここで、図１７に示すフロー図は、図２に示すフロー図においてＳ１０７とＳ１０８との間に接続情報テーブル２６ｅのアクセス回数を０にリセットする処理フローＳ６００を追加したものであるから、その他の処理については図２と同一符号を付し、ここでは簡単な説明に留める。

【００８３】まず、図１７に示すフロー図において、認証・接続情報生成プログラム２０ｅがクライアント１０から要求信号を受信し（Ｓ１０１）、その要求信号に接続情報が含まれていない場合には（Ｓ１０２）、パスワードによるクライアント１０のユーザ認証を行う（Ｓ１０３～Ｓ１０５）。そうして、パスワードによるユーザ認証に成功すれば接続情報を生成して接続情報テーブル２６ｅに登録するとともに（Ｓ１０６，Ｓ１０７）、接続情報テーブル２６ｅのアクセス回数を０にリセットする（Ｓ６００）。

【００８４】また、クライアント１０から受信する要求信号に接続情報が含まれている場合には（Ｓ１０２）、図１８に示すように、その接続情報と接続情報テーブル２６ｅとに基づいてクライアント１０のユーザ認証を行う（Ｓ６０１）。そして、接続情報を用いたクライアント１０のユーザ認証に失敗すれば、クライアント１０とサーバ１２ｅとの間の通信を終了する。

【００８５】一方、接続情報を用いたクライアント１０のユーザ認証に成功すれば、認証・接続情報生成プログラム２０ｅは、次に接続情報テーブル２６ｅに記憶されているアクセス回数の値をインクリメントして接続情報テーブル２６ｅのアクセス回数の値ｎを更新する（Ｓ６０２）。さらに認証・接続情報生成プログラム２０ｅは、パスワードテーブル２４ｅから接続情報変更回数の値Ｋを読み出し（Ｓ６０３）、その値とアクセス回数の値とを比較する（Ｓ６０４）。そして、アクセス回数の値ｎが接続情報変更回数の値Ｋよりも小さな値であれば、認証・接続情報生成プログラム２０ｅは新たな接続情報を生成し（Ｓ６０５）、それを接続情報テーブル２６ｅに格納して接続情報を更新する（Ｓ６０６）。その

後、通常通りサーバプログラム２２へのアクセス処理を行う（Ｓ１０８）。この際、Ｓ１１１においてクライアント１０に送信される接続情報はＳ６０５において新たに生成されたものである。クライアントプログラム１６は、この新たな接続情報をサーバ１２ｅから受信し、記憶手段１８に既に記憶されている古い接続情報を更新する。

【００８６】一方、アクセス回数の値ｎが接続情報変更回数の値Ｋ以上であれば、認証・接続情報生成プログラム２０ｅは接続情報テーブル２６ｅからそのクライアント１０の接続情報を抹消する（Ｓ６０７）。そうして、再びクライアント１０に対してユーザ名とパスワードの送信を要求する（Ｓ１０３）。

【００８７】以上説明した本実施の形態によれば、パスワードによるユーザ認証を行った後のクライアント１０とサーバ１２ｅとのアクセスの回数がカウントされ、その回数が所定回数以上になれば再びクライアント１０に対してパスワードによるユーザ認証が求められる。すなわち、本実施の形態によれば、クライアント１０とサーバ１２ｅとの間で所定回数のアクセスの度にパスワードによるユーザ認証が行われる。この結果、万が一接続情報が他のユーザに漏洩した場合にも、所定回数内に不正アクセスを制限することができる。

【００８８】実施の形態７．図１９は、本発明の実施の形態７に係る通信システムを示す機能ブロック図である。同図に示す通信システムは、上記各実施の形態に係る通信システムに比して、パスワードテーブル２４ｆと接続情報テーブル２６ｆの内容と認証・接続情報生成プログラム２０ｆの処理と、にその特徴を有するものである。そして、クライアント１０の構成とサーバ１２ｆのサーバプログラム２２は、上記各実施の形態に係る通信システムと同様であるので、ここでは同一符号を付して説明を省略する。

【００８９】まず、本実施の形態に係る通信システムのパスワードテーブル２４ｆには、ユーザ名とパスワードとに対応づけて、各ユーザの接続情報削除経過時間が記憶されている。この接続情報削除経過時間は接続情報テーブル２６ｆに記憶されている接続情報を削除する条件を決める設定値であり、図示しない入力手段によりクライアント１０又はサーバ１２ｆのユーザにより予め設定入力される。

【００９０】また、本実施の形態に係る通信システムの接続情報テーブル２６ｆには、実施例３に係る通信システムと同様、ユーザ名と接続情報に対応づけて、各ユーザの接続情報生成時刻が記憶されている。この接続情報生成時刻は接続情報が生成された時刻を表す。

【００９１】一方、本通信システムの認証・接続情報生成プログラム２０ｆは、クライアント１０のアクセスがある毎に接続情報テーブル２６ｆの接続情報生成時刻からそのアクセスの時点までの経過時間を計算する。そして、その計算した経過時間がパスワードテーブル２４ｆに記憶されている接続情報削除経過時間の値に達すれば、接続情報テーブル２６ｆからそのユーザの接続情報を抹消し、再びクライアント１０に対してユーザ名とパスワードの送信を要求する。一方、その計算した経過時間がパスワードテーブル２４ｆに記憶されている接続情報削除経過時間に達していなければ、新たな接続情報を生成してクライアント１０に送信するとともに、接続情報テーブル２６ｆに既に記録されている接続情報の値を新たなものに更新する。

【００９２】本実施の形態においては、パスワードによるクライアント１０のユーザ認証の後、所定時間が経過した場合に、認証・接続情報生成プログラム２０ｆによるクライアント１０のユーザ認証を一旦中止する第３の認証中止手段としても機能する。

【００９３】以下、かかる構成を有する本通信システムの動作について図２０および図２１に示すフロー図に基づいて説明する。ここで、図２０に示すフロー図は、図２に示すフロー図においてＳ１０７とＳ１０８との間に接続情報テーブル２６ｆの接続情報生成時刻を現在時刻に更新する処理フローＳ７００を追加したものであるから、その他の処理については図２と同一符号を付し、ここでは簡単な説明に留める。

【００９４】まず、図２０に示すフロー図において、認証・接続情報生成プログラム２０ｆがクライアント１０から要求信号を受信し（Ｓ１０１）、その要求信号に接続情報が含まれていない場合には（Ｓ１０２）、パスワードによるクライアント１０のユーザ認証を行う（Ｓ１０３～Ｓ１０５）。そうして、パスワードによるユーザ認証に成功すれば接続情報を生成して接続情報テーブル２６ｆに登録するとともに（Ｓ１０６，Ｓ１０７）、接続情報テーブル２６ｆの接続情報生成時刻の値を図示しない内部クロックから出力される現在時刻の値に再設定する（Ｓ７００）。

【００９５】また、クライアント１０から受信する要求信号に接続情報が含まれている場合には（Ｓ１０２）、図２１に示すように、その接続情報と接続情報テーブル２６ｆとに基づいてクライアント１０のユーザ認証を行う（Ｓ７０１）。そして、接続情報を用いたクライアント１０のユーザ認証に失敗すれば、クライアント１０とサーバ１２ｆとの間の通信を終了する。

【００９６】一方、接続情報を用いたクライアント１０のユーザ認証に成功すれば、認証・接続情報生成プログラム２０ｆは、次に接続情報テーブル２６ｆに記憶されている接続情報生成時刻を図示しない内部クロックから出力された現在時刻から減算し、接続情報を生成した時点から現在までの経過時間ｔを導出する（Ｓ７０２）。さらに認証・接続情報生成プログラム２０ｆは、パスワードテーブル２４ｆから接続情報変更経過時間Ｔを読み出し（Ｓ７０３）、その値とＳ７０２で導出した経過時

間ｔの値とを比較する（Ｓ７０４）。

【００９７】そして、経過時間ｔが接続情報変更経過時間Ｔよりも小さな値であれば、認証・接続情報生成プログラム２０ｆは新たな接続情報を生成し（Ｓ７０５）、それを接続情報テーブル２６ｆに格納して接続情報を更新する（Ｓ７０６）。その後、通常通りサーバプログラム２２へのアクセス処理を行う（Ｓ１０８）。この際、Ｓ１１１においてクライアント１０に送信される接続情報はＳ７０５において新たに生成されたものである。クライアントプログラム１６は、この新たな接続情報をサーバ１２ｆから受信し、記憶手段１８に既に記憶されている古い接続情報を更新する。

【００９８】一方、経過時間ｔが接続情報変更経過時間Ｔ以上であれば、認証・接続情報生成プログラム２０ｆは接続情報テーブル２６ｆからそのクライアント１０の接続情報を抹消する（Ｓ７０７）。そうして、再びクライアント１０に対してユーザ名とパスワードの送信を要求する（Ｓ１０３）。

【００９９】以上説明した本実施の形態によれば、パスワードによるユーザ認証を行ってから一定時間が経過すれば再びクライアント１０に対してパスワードによるユーザ認証が求められる。すなわち、本実施の形態によれば、所定時間を経過する度にパスワードによるユーザ認証が行われる。この結果、万が一接続情報が他のユーザに漏洩した場合にも、所定時間内に不正アクセスを制限することができる。

【０１００】実施の形態８．図２２は、本発明の実施の形態８に係る通信システムを示す機能ブロック図である。同図に示す通信システムは、上記実施の形態６に係る通信システムの技術と上記実施の形態７に係る通信システムの技術との組み合わせに係るものであり、パスワードテーブル２４ｇと接続情報テーブル２６ｇの内容と認証・接続情報生成プログラム２０ｇの処理と、にその特徴を有するものである。そして、クライアント１０およびその内部構成とサーバ１２ｇのサーバプログラム２２は、実施の形態１に係る通信システムと同様であるので、ここでは同一符号を付して説明を省略する。

【０１０１】まず、本実施の形態に係る通信システムのパスワードテーブル２４ｇには、ユーザ名とパスワードとに対応づけて、各ユーザの接続情報削除回数と接続情報削除経過時間とが記憶されている。接続情報削除回数と接続情報削除経過時間は接続情報テーブル２６ｇに記憶されている接続情報を削除する条件を決める設定値であり、図示しない入力手段によりクライアント１０又はサーバ１２ｇのユーザにより予め設定入力される。

【０１０２】また、本実施の形態に係る通信システムの接続情報テーブル２６ｇには、ユーザ名と接続情報に対応づけて、実施例６に係る通信システムと同様、各ユーザのアクセス回数が記憶されるとともに、実施例７に係る通信システムと同様、各ユーザの接続情報生成時刻が記憶されている。アクセス回数は新たな接続情報が生成されて接続情報テーブル２６ｇに格納されてから後の、そのクライアント１０のアクセス回数を表す。接続情報生成時刻は接続情報が生成された時刻を表す。

【０１０３】一方、本通信システムの認証・接続情報生成プログラム２０ｇは、クライアント１０のアクセスがある毎に接続情報テーブル２６ｇのアクセス回数の値をインクリメントして更新する。そして、そのアクセス回数がパスワードテーブル２４ｇに記憶されている接続情報削除回数の値に達すれば、接続情報テーブル２６ｇからそのユーザの接続情報を抹消し、再びクライアント１０に対してユーザ名とパスワードの送信を要求する。

【０１０４】また、アクセス回数がパスワードテーブル２４ｇに記憶されている接続情報削除回数に達していない場合でも、接続情報テーブル２６ｇの接続情報生成時刻からそのアクセスの時点までの経過時間を計算し、その計算した経過時間がパスワードテーブル２４ｇに記憶されている接続情報削除経過時間の値に達していれば、接続情報テーブル２６ｇからそのユーザの接続情報を抹消し、再びクライアント１０に対してユーザ名とパスワードの送信を要求する。

【０１０５】一方、アクセス回数がパスワードテーブル２４ｇに記憶されている接続情報削除回数に達しておらず、且つ経過時間がパスワードテーブル２４ｇに記憶されている接続情報削除経過時間に達していなければ、新たな接続情報を生成してクライアント１０に送信するとともに、接続情報テーブル２６ｇに既に記録されている接続情報の値を新たなものに更新する。

【０１０６】以下、かかる構成を有する本通信システムの動作について図２３および図２４に示すフロー図に基づいて説明する。ここで、図２３に示すフロー図は、図２に示すフロー図においてＳ１０７とＳ１０８との間に接続情報テーブル２６ｇのアクセス回数を０にリセットする処理フローＳ８００と接続情報テーブル２６ｇの接続情報生成時刻を現在時刻に更新する処理フローＳ８０１とを追加したものであるから、その他の処理については図２と同一符号を付し、ここでは簡単な説明に留める。

【０１０７】まず、図２３に示すフロー図において、認証・接続情報生成プログラム２０ｇがクライアント１０から要求信号を受信し（Ｓ１０１）、その要求信号に接続情報が含まれていない場合には（Ｓ１０２）、パスワードによるクライアント１０のユーザ認証を行う（Ｓ１０３～Ｓ１０５）。そうして、パスワードによるユーザ認証に成功すれば接続情報を生成して接続情報テーブル２６ｇに登録する（Ｓ１０６，Ｓ１０７）。また、接続情報テーブル２６ｇのアクセス回数を０にリセットするとともに（Ｓ８００）、接続情報テーブル２６ｅの接続情報生成時刻の値を図示しない内部クロックから出力される現在時刻の値に再設定する（Ｓ８０１）。

【０１０８】また、クライアント１０から受信する要求信号に接続情報が含まれている場合には（Ｓ１０２）、図２４に示すように、その接続情報と接続情報テーブル２６ｇとに基づいてクライアント１０のユーザ認証を行う（Ｓ８０２）。そして、接続情報を用いたクライアント１０のユーザ認証に失敗すれば、クライアント１０とサーバ１２ｇとの間の通信を終了する。

【０１０９】一方、接続情報を用いたクライアント１０のユーザ認証に成功すれば、認証・接続情報生成プログラム２０ｇは、次に接続情報テーブル２６ｇに記憶されているアクセス回数の値をインクリメントして接続情報テーブル２６ｇのアクセス回数の値ｎを更新する（Ｓ８０３）。さらに認証・接続情報生成プログラム２０ｇは、パスワードテーブル２４ｇから接続情報削除回数の値Ｋを読み出し（Ｓ８０４）、その値とアクセス回数の値とを比較する（Ｓ８０５）。

【０１１０】そして、アクセス回数の値ｎが接続情報削除回数の値Ｋよりも小さな値であれば、認証・接続情報生成プログラム２０ｇは、次に接続情報テーブル２６ｇに記憶されている接続情報生成時刻を図示しない内部クロックから出力された現在時刻から減算し、接続情報を生成した時点から現在までの経過時間ｔを導出する（Ｓ８０６）。さらに認証・接続情報生成プログラム２０ｇは、パスワードテーブル２４ｇから接続情報削除経過時間Ｔを読み出し（Ｓ８０７）、その値とＳ８０６で導出した経過時間ｔの値とを比較する（Ｓ８０８）。

【０１１１】そして、経過時間ｔが接続情報削除経過時間Ｔよりも小さな値であれば、認証・接続情報生成プログラム２０ｇは新たな接続情報を生成し（Ｓ８０９）、それを接続情報テーブル２６ｇに格納して接続情報を更新する（Ｓ８１０）。その後、通常通りサーバプログラム２２へのアクセス処理を行う（Ｓ１０８）。この際、Ｓ１１１においてクライアント１０に送信される接続情報はＳ８０９において新たに生成されたものである。クライアントプログラム１６は、この新たな接続情報をサーバ１２ｇから受信し、記憶手段１８に既に記憶されている古い接続情報を更新する。

【０１１２】一方、アクセス回数の値ｎが接続情報削除回数の値Ｋ以上である場合、或いは経過時間ｔが接続情報削除経過時間Ｔ以上である場合、認証・接続情報生成プログラム２０ｇは接続情報テーブル２６ｇからそのクライアント１０の接続情報を抹消する（Ｓ８１１）。そうして、再びクライアント１０に対してユーザ名とパスワードの送信を要求する（Ｓ１０３）。

【０１１３】以上説明した本実施の形態によれば、パスワードによるユーザ認証を行ってから一定時間が経過した場合、或いはパスワードによるユーザ認証を行ってから所定回数のアクセスが発生した場合に、再びクライアント１０に対してパスワードによるユーザ認証が求められる。この結果、万が一接続情報が他のユーザに漏洩した場合にも、所定回数と所定時間の内に不正アクセスを制限することができる。

【０１１４】なお、上記説明においては、アクセス回数ｎが接続情報削除回数Ｋ以上である場合又は経過時間ｔが接続情報削除経過時間Ｔ以上である場合のいずれの場合にも接続情報を抹消したが、アクセス回数ｎが接続情報削除回数Ｋ以上である場合であり、且つ経過時間ｔが接続情報削除経過時間Ｔ以上である場合にのみ接続情報を抹消するようにしてもよい。

【０１１５】実施の形態９．本発明の実施の形態９に係る通信システムは上記実施の形態１に係る通信システムと同一の構成であり、ただ、認証・接続情報生成プログラム２０の動作の一部が異なるものである。具体的には、本実施の形態に係る通信システムは、実施の形態１に係る通信システムの動作を示す図２および図３のフロー図において、認証・接続情報生成プログラム２０が図３のフロー図に示す処理に代えて図２５のフロー図に示す処理を実行するものである。これにより、本実施の形態に係る通信システムでは、クライアント１０のユーザが自己に対して発行されている接続情報を自ら強制的に無効化することができる。

【０１１６】すなわち、本実施の形態においては、認証接続情報生成プログラム２０が、クライアント１０から接続情報を無効化すべき旨の所定の要求信号を受信した場合に、認証・接続情報プログラム２０ｄ（認証手段）によるクライアント１０のユーザ認証を中止する第４の認証中止手段としても機能する。

【０１１７】以下、かかる構成を有する本通信システムの動作について図２および図２５に示すフロー図に基づいて説明する。

【０１１８】まず、図２に示すフロー図において、認証・接続情報生成プログラム２０がクライアント１０から要求信号を受信し（Ｓ１０１）、その要求信号に接続情報が含まれている場合には（Ｓ１０２）、図２５に示すように、その接続情報と接続情報テーブル２６とに基づいてクライアント１０のユーザ認証を行う（Ｓ９０１）。そして、接続情報を用いたクライアント１０のユーザ認証に失敗すれば、クライアント１０とサーバ１２との間の通信を終了する。

【０１１９】一方、接続情報を用いたクライアント１０のユーザ認証に成功すれば、認証・接続情報生成プログラム２０は、クライアント１０から受信した要求信号に接続情報削除要求が含まれているかを判断する（Ｓ９０２）。そして、含まれていれば接続情報テーブル２６からそのユーザの接続情報を削除し（Ｓ９０３）、クライアント１０とサーバ１２との間の通信を終了する。一方、クライアント１０から受信した要求信号に接続情報削除要求が含まれていなければ、通常通りサーバプログラム２２へのアクセス処理を行う（Ｓ１０８）。

【０１２０】以上説明した本実施の形態によれば、ユー

ザは接続情報を自らの意志で強制的に無効化することができ、この結果、ユーザが自ら不要と判断する場合に接続情報を無効化して、成りすましによる不正アクセスを防止することができる。

【０１２１】実施の形態１０．図２６は、本発明の実施の形態１０に係る通信システムを示す機能ブロック図である。同図に示す通信システムは、上記各実施の形態に係る通信システムに比して、クライアント１０に自動アクセスプログラム２８が備えられている点に特徴を有する。この自動アクセスプログラム２８は、認証・接続情報生成プログラム２０からクライアントプログラム１６が受信する実行プログラム（アプレット）であり、クライアントプログラム１６の通信機能を制御することにより一定時間毎にサーバ１２に自動アクセスするものである。なお、クライアントプログラム１６とサーバの構成は、上記各実施の形態に係る通信システムと同様であるので、ここでは同一符号を付して説明を省略する。

【０１２２】本実施の形態においては、自動アクセスプログラム２８と該自動アクセスプログラム２８をクライアント１０に送信する認証・接続情報生成プログラム２０とが、接続情報を用いた一定時間毎のクライアント１０からサーバ１２へのアクセスを発生させるクライアントサーバ間アクセス発生手段として機能する。

【０１２３】以下、かかる構成を有する本通信システムの動作について図２７および図２８に示すフロー図に基づいて説明する。ここで、図２７に示すフロー図は、図２に示すフロー図においてＳ１１１の後に自動アクセスプログラム２８をクライアント１０に送信する処理フローＳ１１２を追加したものであるから、その他の処理については図２と同一符号を付し、ここでは簡単な説明に留める。

【０１２４】図２７に示すように、まず、サーバ１２では、クライアント１０から受信した要求信号に接続情報が含まれていなければ、認証・接続情報生成プログラム２０がクライアント１０に対してユーザ名とパスワードを要求する（Ｓ１０３）。これに対してクライアント１０からユーザ名とパスワードを受信すれば（Ｓ１０４）、次に認証・接続情報生成プログラム２０は、その受信したユーザ名およびパスワードとパスワードテーブル２４とに基づいて、クライアント１０のユーザ認証を行う。認証・接続情報生成プログラム２０がパスワードテーブル２４によるクライアント１０のユーザ認証に成功すれば（Ｓ１０５）、接続情報を生成し（Ｓ１０６）、その接続情報を接続情報テーブル２６にユーザ名とともに追加記録する（Ｓ１０７）。次に、認証・接続情報生成プログラム２０は、サーバプログラム２２にユーザ名等のユーザ情報を送信するとともに（Ｓ１０８）、サーバ情報を獲得するための要求信号を送信する（Ｓ１０９）。そして、認証・接続情報生成プログラム２０は、Ｓ１０６で生成した接続情報をクライアント１０に送信するとともに（Ｓ１１０）、サーバプログラム２２から受信したサーバ情報をクライアント１０に送信する（Ｓ１１１）。クライアントプログラム１６は、サーバ情報を受信したときに未だ自動アクセスプログラム２８を受信していなければ、サーバ１２に対して自動アクセスプログラム２８の送信を要求する。これに対し、サーバ１２は要求された自動アクセスプログラム２８をクライアント１０に送信する（Ｓ１１２）。たとえば、WWWシステムにおいては、クライアントプログラム１６は、サーバ情報であるハイパーテキスト中にアプレットをサーバ１２から取得すべき旨のタグ情報が含まれている場合に、そのタグ情報にしたがってサーバ１２から自動アクセスプログラム２８であるアプレットを取得する。

【０１２５】この自動アクセスプログラム２８は、クライアントプログラム１６の通信機能を制御することにより、一定時間毎にサーバ１２にアクセスを行うものであり、その際、サーバ情報を要求する旨の要求信号とともにクライアント１０のメモリに格納されている接続情報をサーバ１２に送信する。

【０１２６】サーバ１２では、この自動アクセスプログラム２８からの接続情報を伴う要求信号を受信すれば、認証・接続情報生成プログラム２０が接続情報テーブル２６を用いたクライアント１０のユーザ認証を行う（Ｓ１００１）。そして、クライアント１０のユーザ認証に失敗すれば、クライアント１０とサーバ１２との間の通信を終了する。一方、認証・接続情報生成プログラム２０は、接続情報テーブル２６によるクライアント１０のユーザ認証に成功すれば、新たな接続情報を生成し（Ｓ１００２）、その接続情報を更新すべく新たな接続情報を接続情報テーブル２６に上書き記憶させる（Ｓ１００３）。

【０１２７】以上説明した本実施の形態によれば、自動アクセスプログラム２８により一定の時間間隔でクライアント１０とサーバ１２との間のアクセスが発生する。そして、例えばアクセスの度に接続情報を更新することにより、接続情報の盗聴の可能性を少なくすることができるとともに、万が一接続情報が漏洩した場合にもその接続情報による不正アクセスを抑制することができる。

【０１２８】なお、以上説明した通信システムは種々の変形実施が可能である。例えば、実施の形態５に係る通信システムの技術を組み合わせることにより、前回アクセス時刻から一定時間以上経過した後にクライアント１０からアクセスがあれば、接続情報テーブル２６からそのクライアント１０の接続情報を抹消して、再びユーザ名とパスワードをユーザに要求することもできる。また、最後のアクセス時刻から一定時間以上経過すれば、そのユーザの接続情報を接続情報テーブル２６から自動的に抹消するようにしてもよい。いずれにしても、最終アクセス時刻から一定時間以上経過すれば、そのユーザ

には再びユーザ名とパスワードによるユーザ認証を行うようにすれば、さらに確実になりすまし等の不正アクセスを防ぐことができる。

【０１２９】また、以上説明した通信システムは、サーバ１２からクライアント１０に自動アクセスプログラム２８を送信するものであったが、例えばWWWシステムにおいては、サーバ１２からクライアント１０に送信するハイパーテキスト（サーバ情報）に、同じハイパーテキストを所定時間後に再び取得すべき旨のタグ情報を含ませ、一方、クライアント１０にてこのタグ情報を解釈して、直前に受信したハイパーテキストと同じハイパーテキストを所定時間後に再びサーバ１２から取得するようにしてもよい。こうしても、クライアント１０とサーバ１２とのアクセスを所定時間毎に発生させることができ、成りすまし等の不正アクセスを防止することができる。

【０１３０】実施の形態１１．図２９は、本発明の実施の形態１１に係る通信システムを示す機能ブロック図である。同図に示す通信システムは、上記実施の形態１０に係る通信システムに比して、クライアント１０にクライアントプログラム１６とクライアントプログラム１６ａとが備えられ、自動アクセスプログラム２８はクライアントプログラム１６ａの通信機能を用いてサーバ１２に自動アクセスする点に特徴を有する。そして、その他の構成は、上記各実施の形態に係る通信システムと同様であるので、ここでは同一符号を付して説明を省略する。

【０１３１】図３０および図２８は本実施の形態に係る通信システムの動作を説明するフロー図である。ここで、図３０に示すフロー図は、図２７に示すフロー図においてＳ１１１の後に自動アクセスプログラム２８をクライアント１０に送信するとともにクライアントプログラム１６ａの起動命令をクライアント１０に送信する処理フローＳ１１３を追加したものであり、その他の処理については図２７と同一符号を付している。また、Ｓ１０２において、認証・接続情報生成プログラム２０がクライアント１０から受信した要求信号に接続情報が含まれていないと判断すれば、該認証・接続情報生成プログラム２０は既に示した図２８のフロー図に処理を移行する。

【０１３２】これらの図に示すように、サーバ１２の認証・接続情報生成プログラム２０は、パスワードテーブル２４によるクライアント１０のユーザ認証に成功した場合（Ｓ１０５）、或いは接続情報テーブル２６によるクライアント１０のユーザ認証に成功した場合（Ｓ１００１）、要求のあったサーバ情報をクライアント１０に送信し（Ｓ１１１）、その際、自動アクセスプログラム２８とクライアントプログラム１６ａの起動命令とをクライアント１０に送信する（Ｓ１１３）。そうして、クライアント１０では、これら自動アクセスプログラム２８とクライアントプログラム１６ａの起動命令とを受信すれば、クライアントプログラム１６がクライアントプログラム１６ａを起動するとともに、受信した自動アクセスプログラム２８をそのクライアントプログラム１６ａの子プロセスとして実行する。そして、自動アクセスプログラム２８は、所定時間後、クライアントプログラム１６ａの有する通信機能を用いてクライアントプログラム１６が直前に受信しているサーバ情報と同じサーバ情報を要求する旨の要求信号をサーバ１２に送信する。

【０１３３】サーバ１２では、この自動アクセスプログラム２８からの接続情報を伴う要求信号を受信すれば、認証・接続情報生成プログラム２０が接続情報テーブル２６を用いたクライアント１０のユーザ認証を行う（Ｓ１００１）。そして、クライアント１０のユーザ認証に失敗すれば、クライアント１０とサーバ１２との間の通信を終了する。一方、認証・接続情報生成プログラム２０は、接続情報テーブル２６によるクライアント１０のユーザ認証に成功すれば、新たな接続情報を生成し（Ｓ１００２）、その接続情報を更新すべく新たな接続情報を接続情報テーブル２６に上書き記憶させる（Ｓ１００３）。

【０１３４】以上説明した本実施の形態によれば、ユーザが実際に操作するクライアントプログラムと自動アクセスプログラム２８が自動アクセスに用いるクライアントプログラムとを分けることができ、この結果、自動アクセスによりユーザが操作するクライアントプログラムがロックすることを防ぐことができる。したがって、本実施の形態によれば、例えば、ユーザが他のサーバ情報を要求する旨の新たな要求信号をサーバ１２に送信したい場合に、自動アクセスプログラム２８がクライアントプログラム１６を使用していて直ちに送信することができない、という事態を回避することができる。

【０１３５】実施の形態１２．図３１は、本発明の実施の形態１２に係る通信システムを示す機能ブロック図である。同図に示す通信システムは、実施の形態１に係る通信システムに比して、クライアント１０に暗号プログラム３０が備えられている点、および認証・接続情報生成プログラム２０ｈがこの暗号プログラム３０による暗号化をデコードする機能を有する点に特徴を有するものである。ここで、暗号プログラム３０は、サーバ１２に対してユーザ名とパスワードを送信する際に、それらを暗号化するプログラムである。すなわち、本実施の形態においては、認証・接続情報生成プログラム２０ｈが、クライアント１０から暗号化されたパスワードが送信された場合に、該パスワードを復号化する復号化手段としても機能する。その他の構成は、実施の形態１に係る通信システムと同様であるので、ここでは同一符号を付して説明を省略する。

【０１３６】図３２および図３は本実施の形態に係る通信システムの動作を説明するフロー図である。ここで、

図３２に示すフロー図は、図２に示すフロー図においてＳ１０４に代えて暗号プログラム３０で暗号化されたユーザ名およびパスワードを受信する処理フローＳ１２００を設け、さらに、そのユーザ名とパスワードとを復号する処理フローＳ１２０１を追加したものであり、その他の処理については図２と同一符号を付している。また、Ｓ１０２において、サーバ１２の認証・接続情報生成プログラム２０ｈがクライアント１０から受信した要求信号に接続情報が含まれていないと判断すれば、該認証・接続情報生成プログラム２０ｈは既に示した図３のフロー図に処理を移行する。

【０１３７】これらの図において、クライアント１０から受信する要求信号に接続情報が含まれていなければ、サーバ１２の認証・接続情報生成プログラム２０ｈはクライアント１０に対してユーザ名とパスワードとを要求する信号を送信する（Ｓ１０３）。これに対してクライアント１０では、クライアントプログラム１６が暗号プログラム３０を用いてユーザ名とパスワードとを暗号化する。そして、クライアントプログラム１６は、その暗号化したユーザ名とパスワードとをサーバ１２に送信する。

【０１３８】暗号化したユーザ名とパスワードとを受信すれば（Ｓ１２００）、サーバ１２の認証・接続情報生成プログラム２０ｈは、これら情報に復号化処理を施して、ユーザ名とパスワードとを取得する（Ｓ１２０１）。そして、これらの情報とパスワードテーブル２４とを用いてクライアント１０のユーザ認証を行う（Ｓ１０５）。

【０１３９】以上説明した本実施の形態によれば、第一段の認証情報として用いるユーザ名およびパスワードを暗号化して送受信することができるため、さらに確実にパスワードの漏洩を防止することができる。

【０１４０】なお、以上説明した本実施の形態に係る通信システムは種々の変形実施が可能である。たとえば上記説明ではクライアント１０のユーザ名とパスワードの双方を暗号プログラム３０により暗号化したが、パスワードだけを暗号化することにしてもよい。

【０１４１】

【発明の効果】本発明によれば、パスワードによるユーザ認証に成功した場合に、以降、接続情報によるユーザ認証ができるようにしたため、パスワードがネットワーク上に送出される機会を減少させることができ、パスワード漏洩による不正アクセスの可能性を減少させることができる。

【０１４２】また、本発明によれば、クライアントから同一の接続情報を所定回数以上受信した場合、或いは接続情報の生成から所定時間が経過した場合に接続情報を更新するようにしたので、接続情報が盗聴された場合にもその接続情報を用いた不正アクセスの機会を奪うことができる。

【０１４３】また、本発明によれば、１）前回のアクセスの時点から所定時間が経過しても再び同じクライアントからのアクセスがない場合、２）パスワードによるユーザ認証の後、所定回数以上そのクライアントからアクセスがあった場合又は所定時間が経過した場合、３）クライアントから接続情報を無効化すべき旨の所定の要求信号を受信した場合に、生成済みの接続情報を無効化するようにしたので、接続情報が盗聴される可能性を少なくすることができるとともに、接続情報が盗聴された場合にもその接続情報を用いた不正アクセスの機会を奪うことができる。

【０１４４】また、本発明によれば、接続情報を用いたクライアントからサーバへのアクセスを一定時間毎に発生させるようにしたので、ユーザによるアクセスを待たずとも接続情報を更新させることができる。これにより、接続情報の漏洩の可能性を少なくすることができる。この際、本発明によれば、接続情報を用いたクライアントからサーバへの上記一定時間毎のアクセスを本体たるクライアントのプロセスとは別プロセスにて行うようにしたので、本体たるクライアントのプロセスの動作を確保することができる。

【０１４５】さらに、本発明によれば、クライアントからサーバへのパスワードの送信に際して、それを暗号化して送受することができるため、パスワードの漏洩を防止することができる。

【図面の簡単な説明】

【図１】　本発明の実施の形態１に係る通信システムを示す機能ブロック図である。

【図２】　本発明の実施の形態１に係る通信システムの動作を説明するフロー図である。

【図３】　本発明の実施の形態１に係る通信システムの動作を説明するフロー図である。

【図４】　本発明の実施の形態２に係る通信システムを示す機能ブロック図である。

【図５】　本発明の実施の形態２に係る通信システムの動作を説明するフロー図である。

【図６】　本発明の実施の形態２に係る通信システムの動作を説明するフロー図である。

【図７】　本発明の実施の形態３に係る通信システムを示す機能ブロック図である。

【図８】　本発明の実施の形態３に係る通信システムの動作を説明するフロー図である。

【図９】　本発明の実施の形態３に係る通信システムの動作を説明するフロー図である。

【図１０】　本発明の実施の形態４に係る通信システムを示す機能ブロック図である。

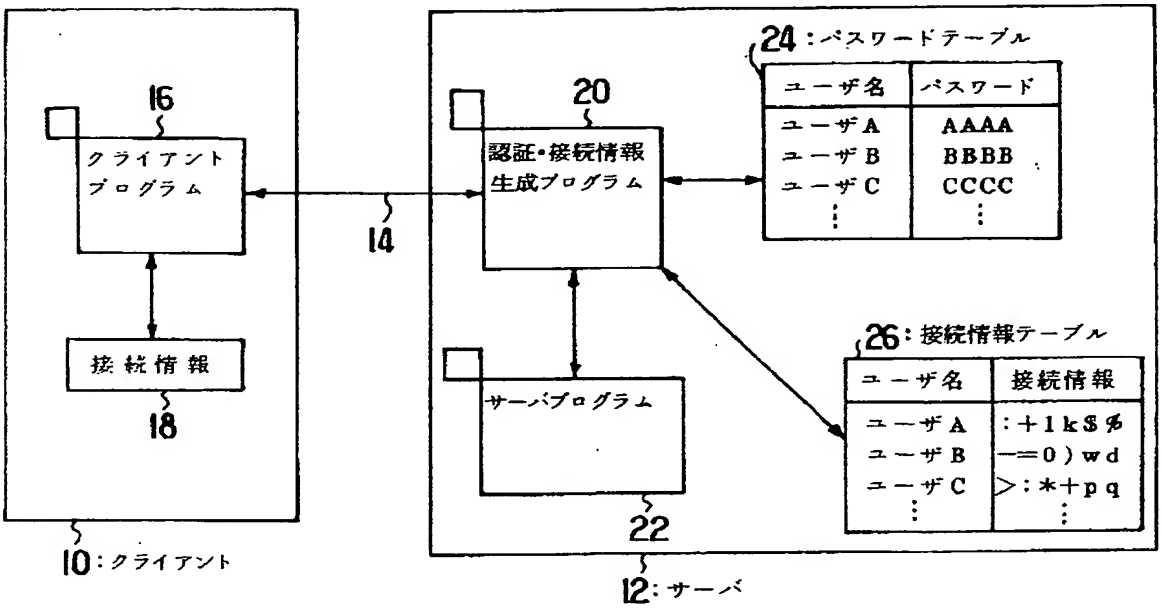
【図１１】　本発明の実施の形態４に係る通信システムの動作を説明するフロー図である。

【図１２】　本発明の実施の形態４に係る通信システムの動作を説明するフロー図である。

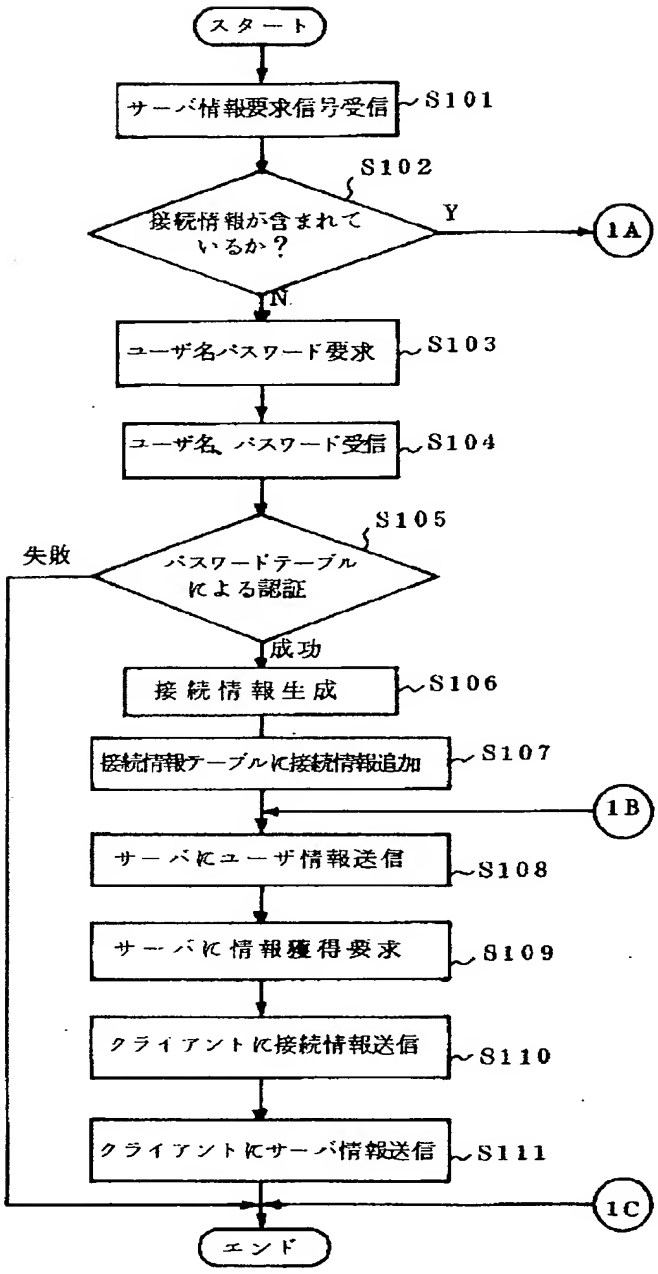
31　　32

【図１３】　本発明の実施の形態５に係る通信システムを示す機能ブロック図である。
【図１４】　本発明の実施の形態５に係る通信システムの動作を説明するフロー図である。
【図１５】　本発明の実施の形態５に係る通信システムの動作を説明するフロー図である。
【図１６】　本発明の実施の形態６に係る通信システムを示す機能ブロック図である。
【図１７】　本発明の実施の形態６に係る通信システムの動作を説明するフロー図である。
【図１８】　本発明の実施の形態６に係る通信システムの動作を説明するフロー図である。
【図１９】　本発明の実施の形態７に係る通信システムを示す機能ブロック図である。
【図２０】　本発明の実施の形態７に係る通信システムの動作を説明するフロー図である。
【図２１】　本発明の実施の形態７に係る通信システムの動作を説明するフロー図である。
【図２２】　本発明の実施の形態８に係る通信システムを示す機能ブロック図である。
【図２３】　本発明の実施の形態８に係る通信システムの動作を説明するフロー図である。
【図２４】　本発明の実施の形態８に係る通信システムの動作を説明するフロー図である。
【図２５】　本発明の実施の形態９に係る通信システムの動作を説明するフロー図である。
【図２６】　本発明の実施の形態１０に係る通信システムを示す機能ブロック図である。
【図２７】　本発明の実施の形態１０に係る通信システムの動作を説明するフロー図である。
【図２８】　本発明の実施の形態１０に係る通信システムの動作を説明するフロー図である。
【図２９】　本発明の実施の形態１１に係る通信システムを示す機能ブロック図である。
【図３０】　本発明の実施の形態１１に係る通信システムの動作を説明するフロー図である。
【図３１】　本発明の実施の形態１２に係る通信システムを示す機能ブロック図である。
【図３２】　本発明の実施の形態１２に係る通信システムの動作を説明するフロー図である。
【符号の説明】
１０　クライアント、１２，１２ａ～１２ｇ　サーバ、１４　通信手段、１６，１６ａ　クライアントプログラム、１８　記憶手段、２０，２０ａ～２０ｈ認証・接続情報生成プログラム、２２　サーバプログラム、２４，２４ａ～２４ｇ　パスワードテーブル、２６，２６ａ～２６ｇ　接続情報テーブル、２８　自動アクセスプログラム、３０　暗号プログラム。

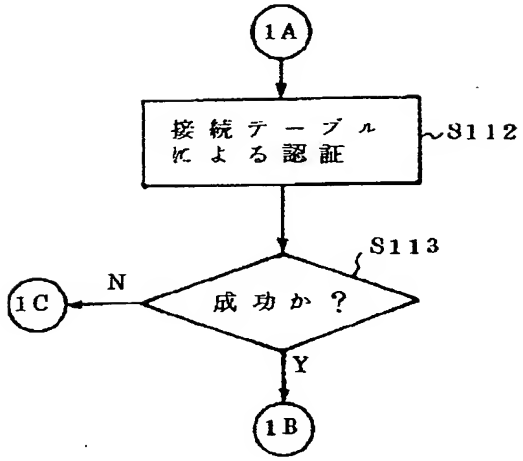
【図１】



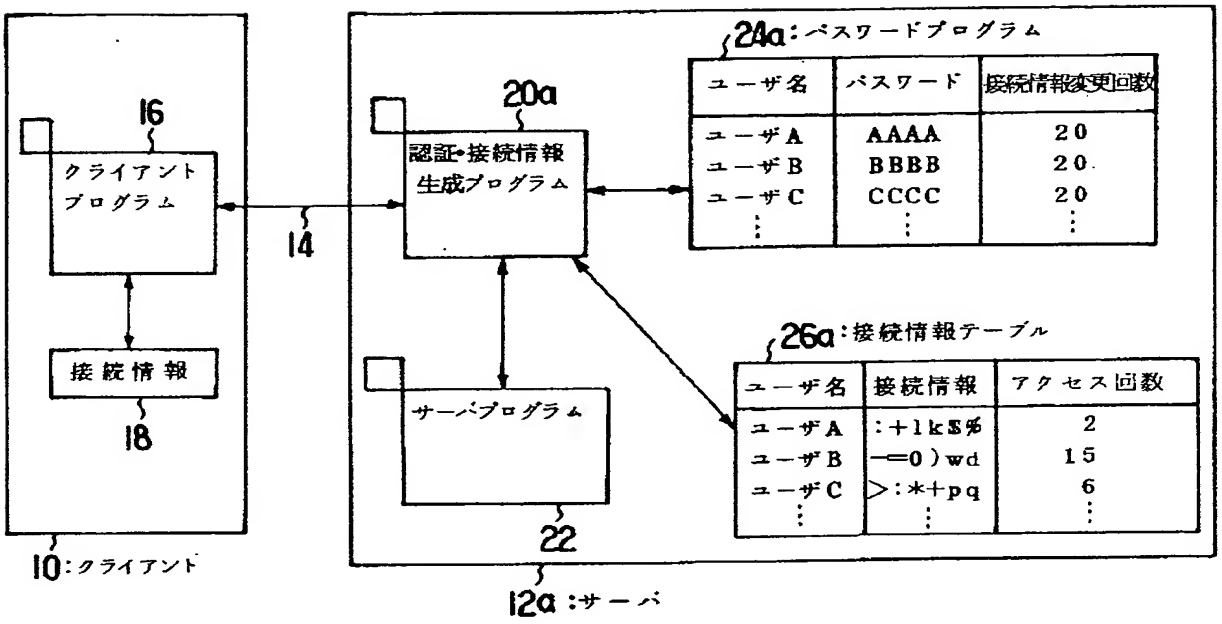
【図２】


スタート
サーバ情報要求信号受信
S101
S102
接続情報が含まれているか？
Y
1A
N
ユーザ名パスワード要求
S103
ユーザ名、パスワード受信
S104
S105
失敗
パスワードテーブルによる認証
成功
接続情報生成
S106
接続情報テーブルに接続情報追加
S107
1B
サーバにユーザ情報送信
S108
サーバに情報獲得要求
S109
クライアントに接続情報送信
S110
クライアントにサーバ情報送信
S111
1C
エンド

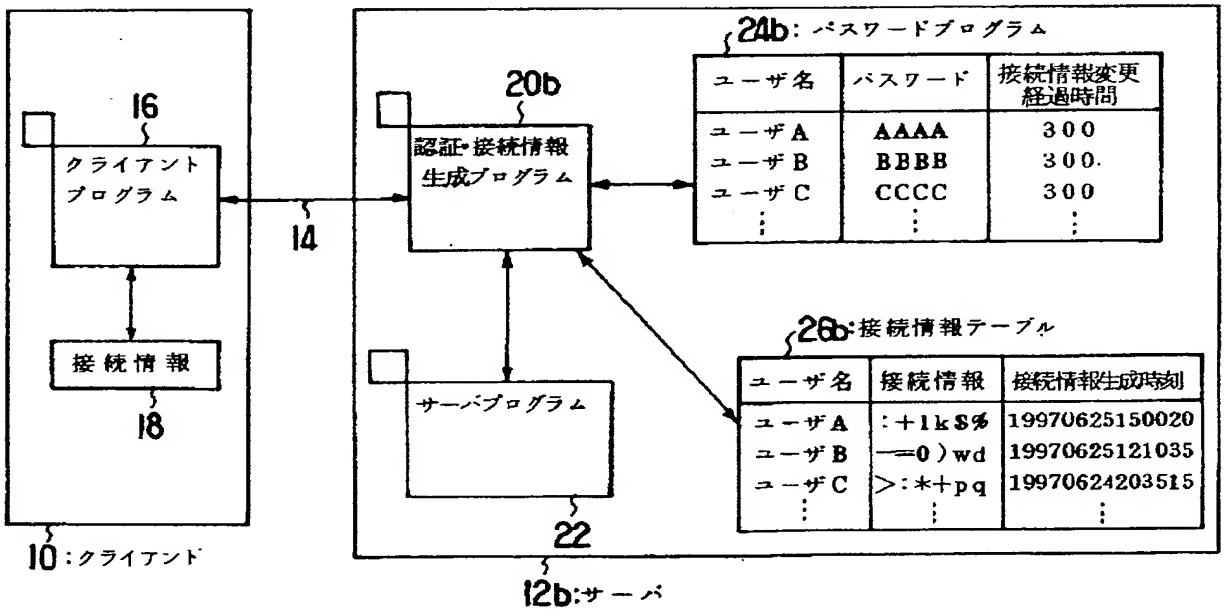
【図３】


1A
接続テーブルによる認証
S112
S113
1C
N
成功か？
Y
1B

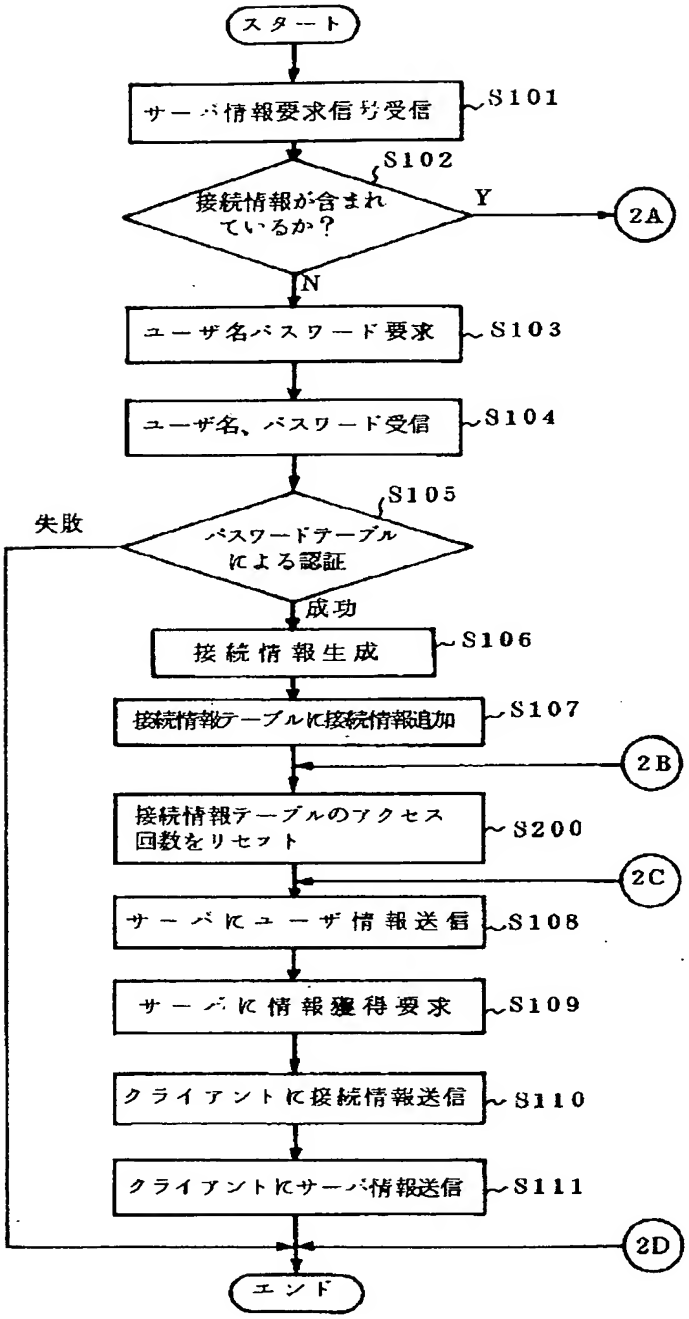
【図４】


24a:パスワードプログラム
ユーザ名
パスワード
接続情報変更回数
ユーザA
ユーザB
ユーザC
AAAA
BBBB
CCCC
20
20
20
20a
認証・接続情報生成プログラム
16
クライアントプログラム
14
接続情報
18
サーバプログラム
22
26a:接続情報テーブル
ユーザ名
接続情報
アクセス回数
ユーザA
ユーザB
ユーザC
2
15
6
10:クライアント
12a:サーバ

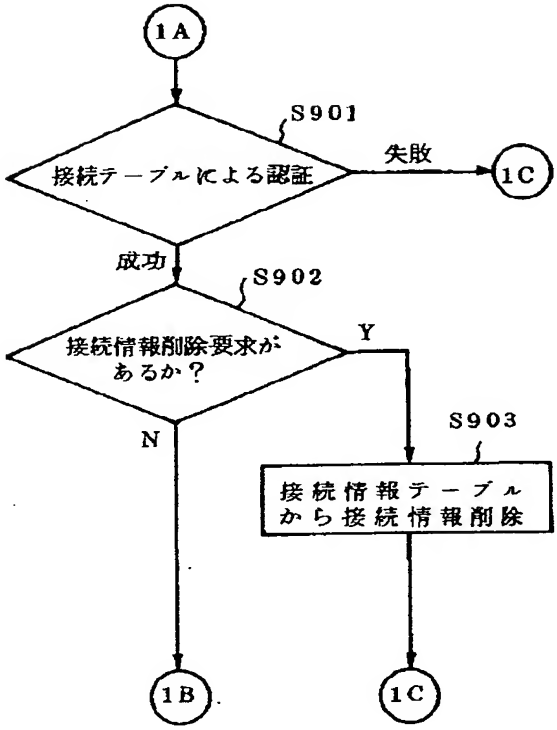
【図７】


24b:パスワードプログラム
ユーザ名
パスワード
接続情報変更経過時間
ユーザA
ユーザB
ユーザC
AAAA
BBBB
CCCC
300
300
300
20b
認証・接続情報生成プログラム
16
クライアントプログラム
14
接続情報
18
サーバプログラム
22
26b:接続情報テーブル
ユーザ名
接続情報
接続情報生成時刻
ユーザA
ユーザB
ユーザC
19970625150020
19970625121035
19970624203515
10:クライアント
12b:サーバ

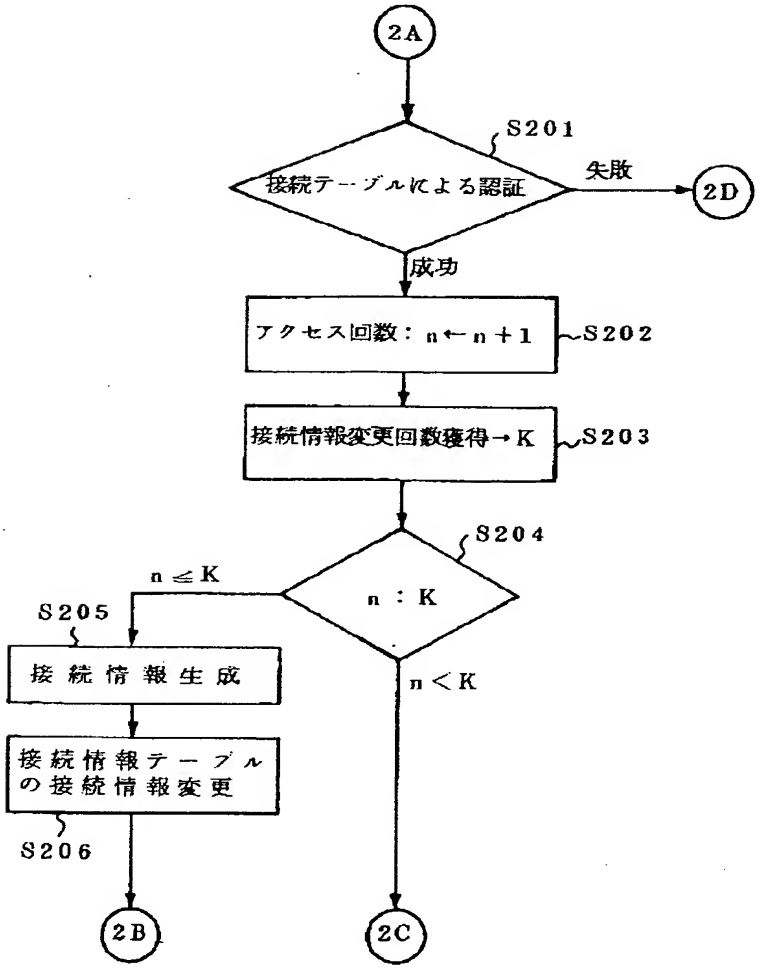
【図5】


スタート
サーバ情報要求信号受信
S101
S102
接続情報が含まれているか？
Y
2A
N
ユーザ名パスワード要求
S103
ユーザ名、パスワード受信
S104
S105
失敗
パスワードテーブルによる認証
成功
接続情報生成
S106
接続情報テーブルに接続情報追加
S107
2B
接続情報テーブルのアクセス回数をリセット
S200
2C
サーバにユーザ情報送信
S108
サーバに情報獲得要求
S109
クライアントに接続情報送信
S110
クライアントにサーバ情報送信
S111
2D
エンド

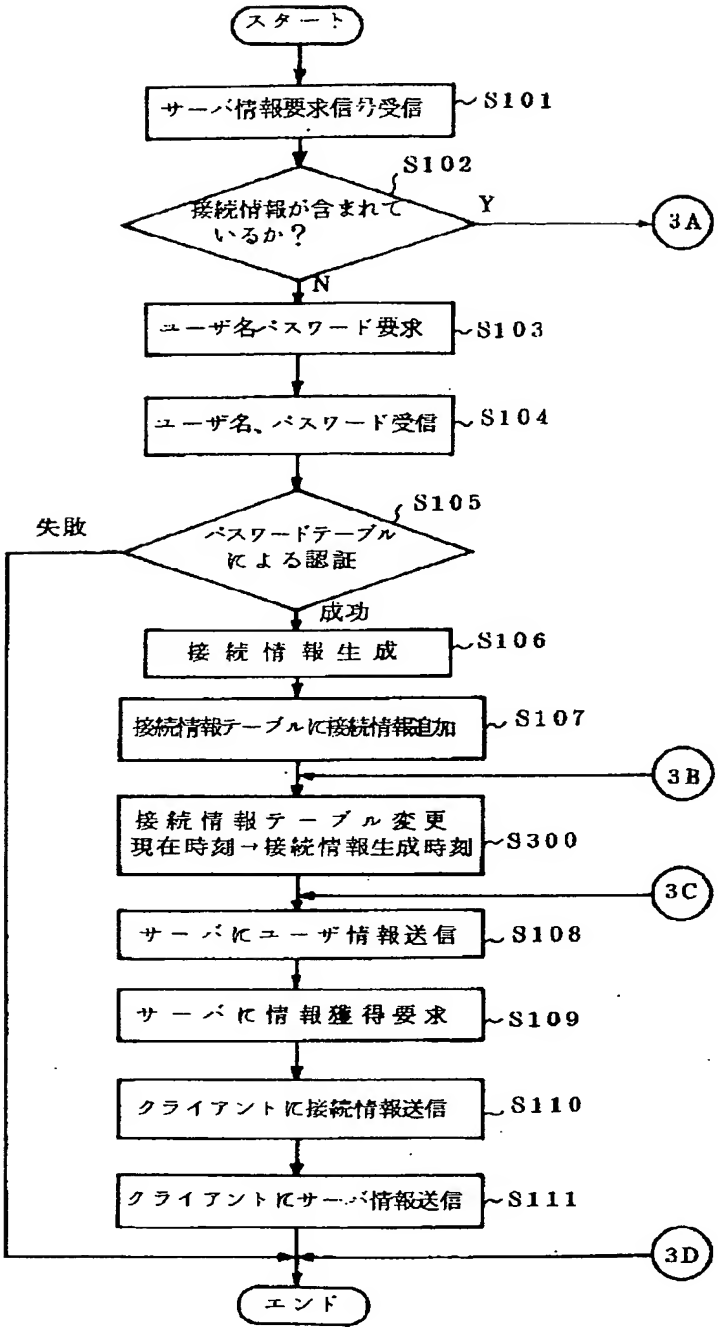
【図25】


1A
S901
接続テーブルによる認証
失敗
1C
成功
S902
接続情報削除要求があるか？
Y
S903
接続情報テーブルから接続情報削除
N
1B
1C

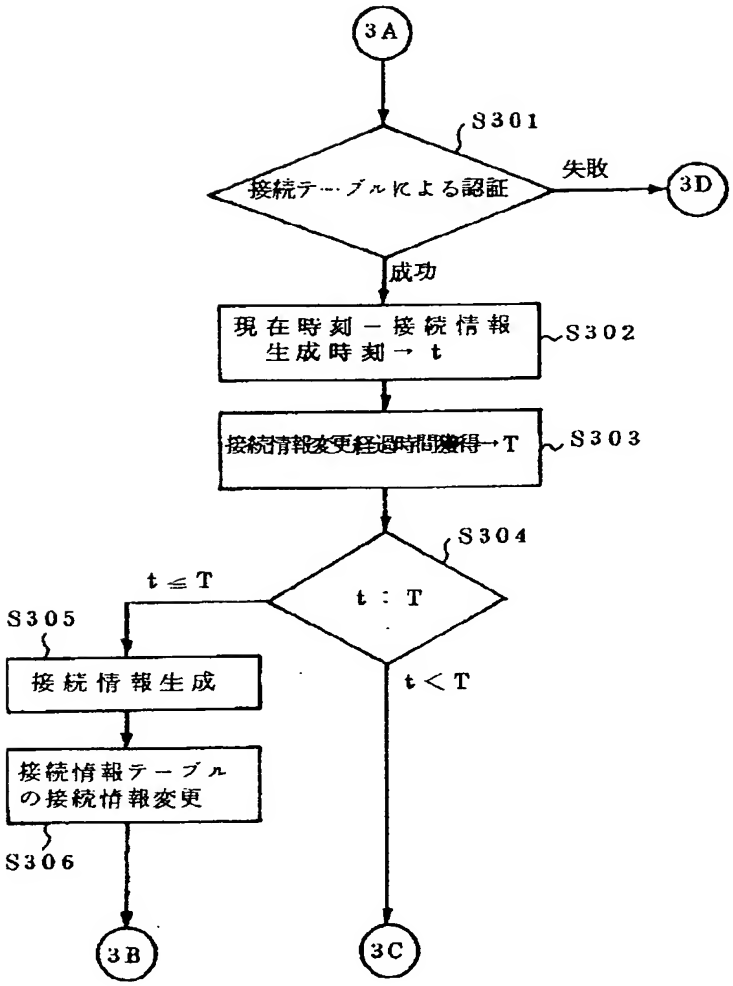
【図６】


2A
S201
接続テーブルによる認証
失敗
2D
成功
アクセス回数：n←n＋1
S202
接続情報変更回数獲得→K
S203
S204
n：K
n≦K
S205
接続情報生成
接続情報テーブルの接続情報変更
S206
n＜K
2B
2C

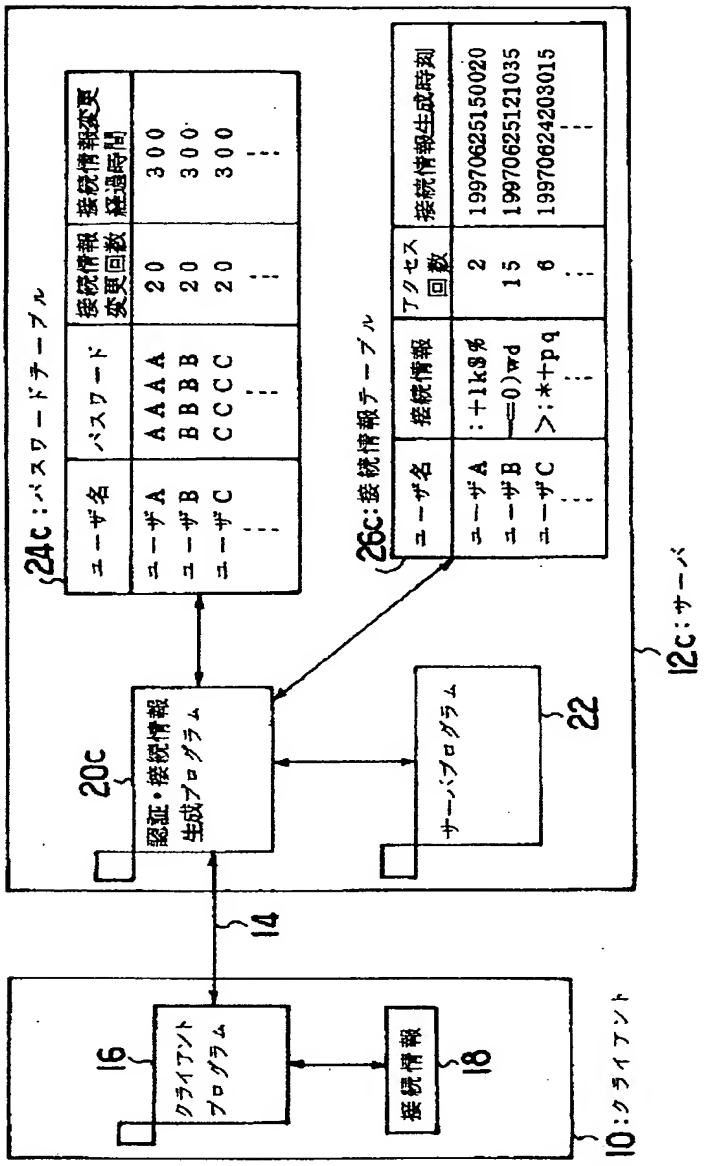
【図８】


スタート
サーバ情報要求信号受信
S101
S102
接続情報が含まれているか？
Y
3A
N
ユーザ名パスワード要求
S103
ユーザ名、パスワード受信
S104
S105
パスワードテーブルによる認証
失敗
成功
接続情報生成
S106
接続情報テーブルに接続情報追加
S107
3B
接続情報テーブル変更
現在時刻→接続情報生成時刻
S300
3C
サーバにユーザ情報送信
S108
サーバに情報獲得要求
S109
クライアントに接続情報送信
S110
クライアントにサーバ情報送信
S111
3D
エンド

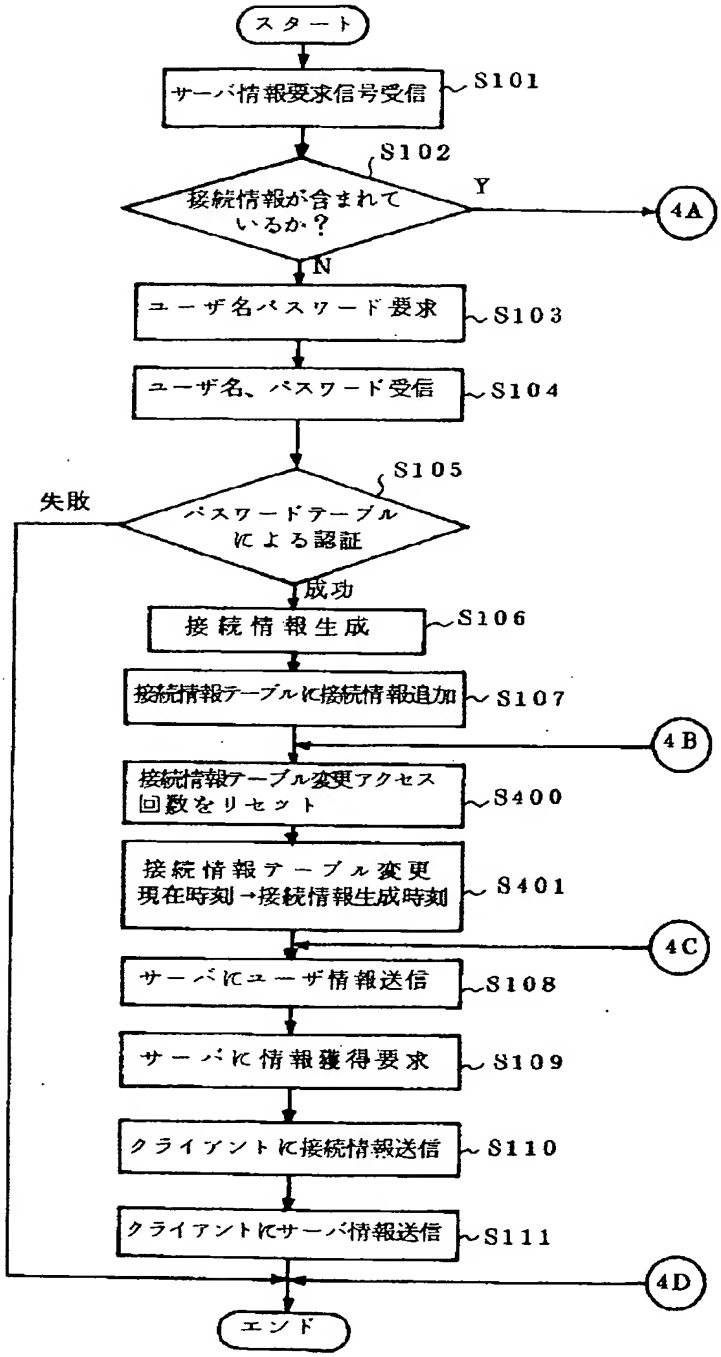
【図９】


3A
S301
接続テーブルによる認証
失敗
3D
成功
現在時刻－接続情報生成時刻→t
S302
接続情報変更経過時間獲得→T
S303
S304
t：T
t≦T
S305
接続情報生成
接続情報テーブルの接続情報変更
S306
t＜T
3B
3C

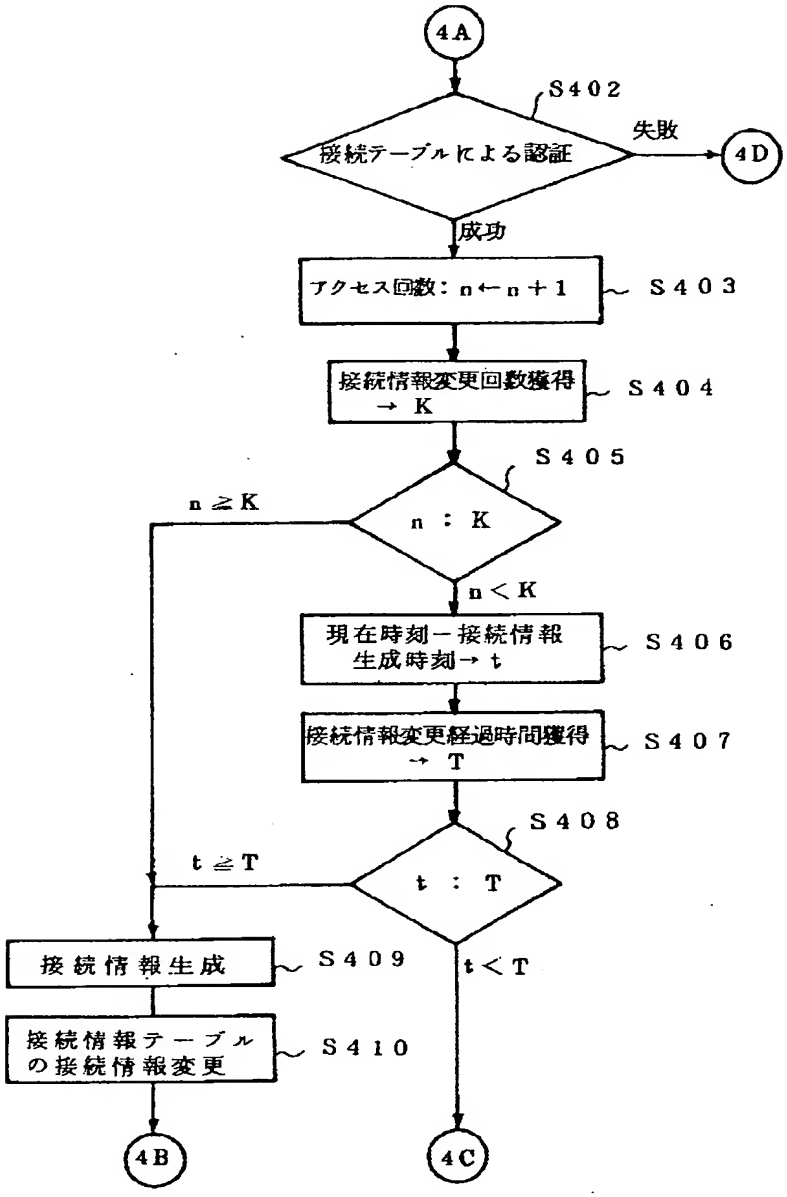
【図１０】


24c：パスワードテーブル
ユーザ名
パスワード
接続情報変更回数
接続情報変更経過時間
ユーザA
AAAA
20
300
ユーザB
BBBB
20
300
ユーザC
CCCC
20
300
26c：接続情報テーブル
ユーザ名
接続情報
アクセス回数
接続情報生成時刻
ユーザA
:+1k8%
2
19970625150020
ユーザB
=0)wd
15
19970625121035
ユーザC
>:*+pq
6
19970624203015
20c
認証・接続情報生成プログラム
22
サーバプログラム
12c：サーバ
14
16
クライアントプログラム
接続情報
18
10：クライアント

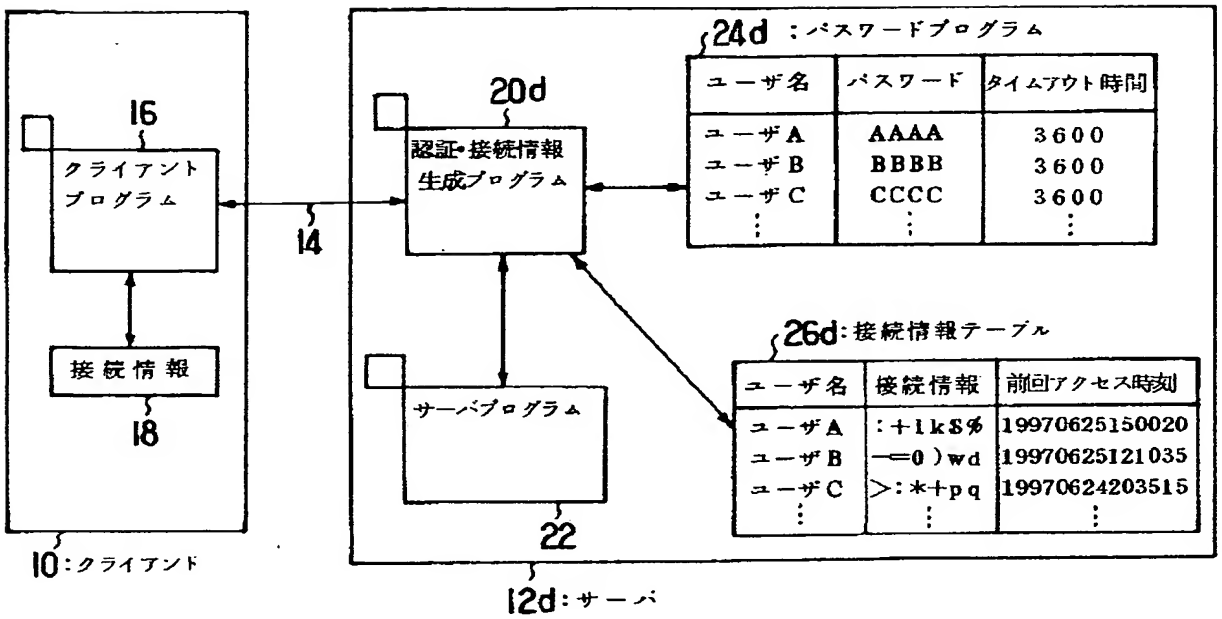
【図１１】


スタート
サーバ情報要求信号受信
S101
S102
接続情報が含まれているか？
Y
4A
N
ユーザ名パスワード要求
S103
ユーザ名、パスワード受信
S104
S105
パスワードテーブルによる認証
失敗
成功
接続情報生成
S106
接続情報テーブルに接続情報追加
S107
4B
接続情報テーブル変更アクセス回数をリセット
S400
接続情報テーブル変更現在時刻→接続情報生成時刻
S401
4C
サーバにユーザ情報送信
S108
サーバに情報獲得要求
S109
クライアントに接続情報送信
S110
クライアントにサーバ情報送信
S111
4D
エンド

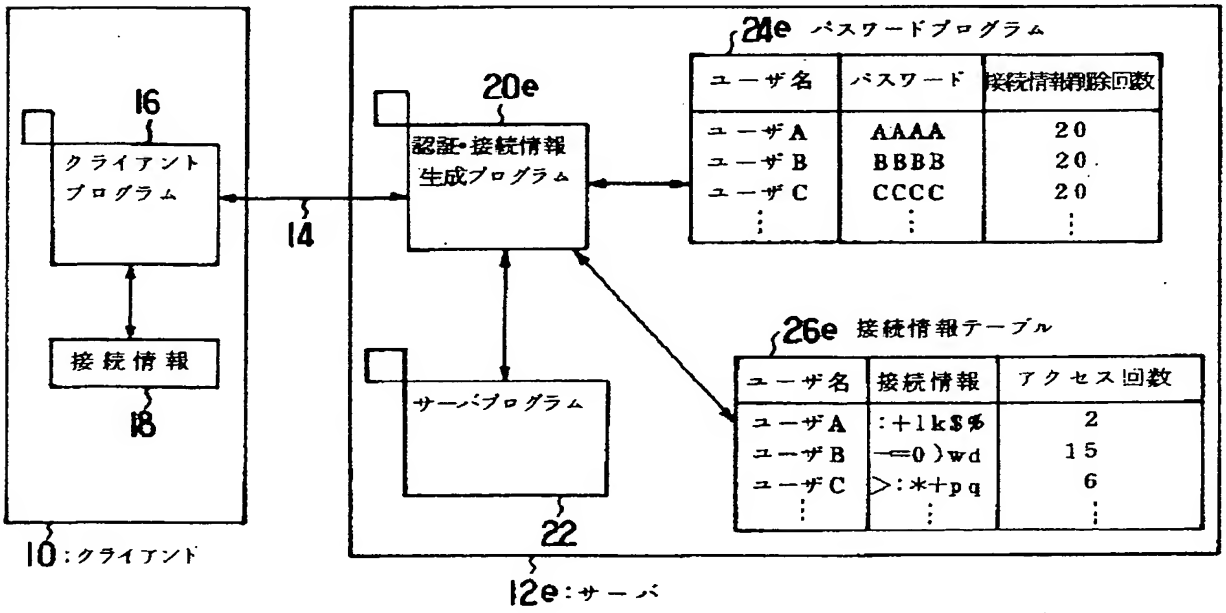
【図１２】


4A
S402
接続テーブルによる認証
失敗
4D
成功
アクセス回数：n←n＋1
S403
接続情報変更回数獲得
→ K
S404
S405
n ： K
n ≧ K
n ＜ K
現在時刻－接続情報
生成時刻→ t
S406
接続情報変更経過時間獲得
→ T
S407
S408
t ： T
t ≧ T
t ＜ T
接続情報生成
S409
接続情報テーブル
の接続情報変更
S410
4B
4C

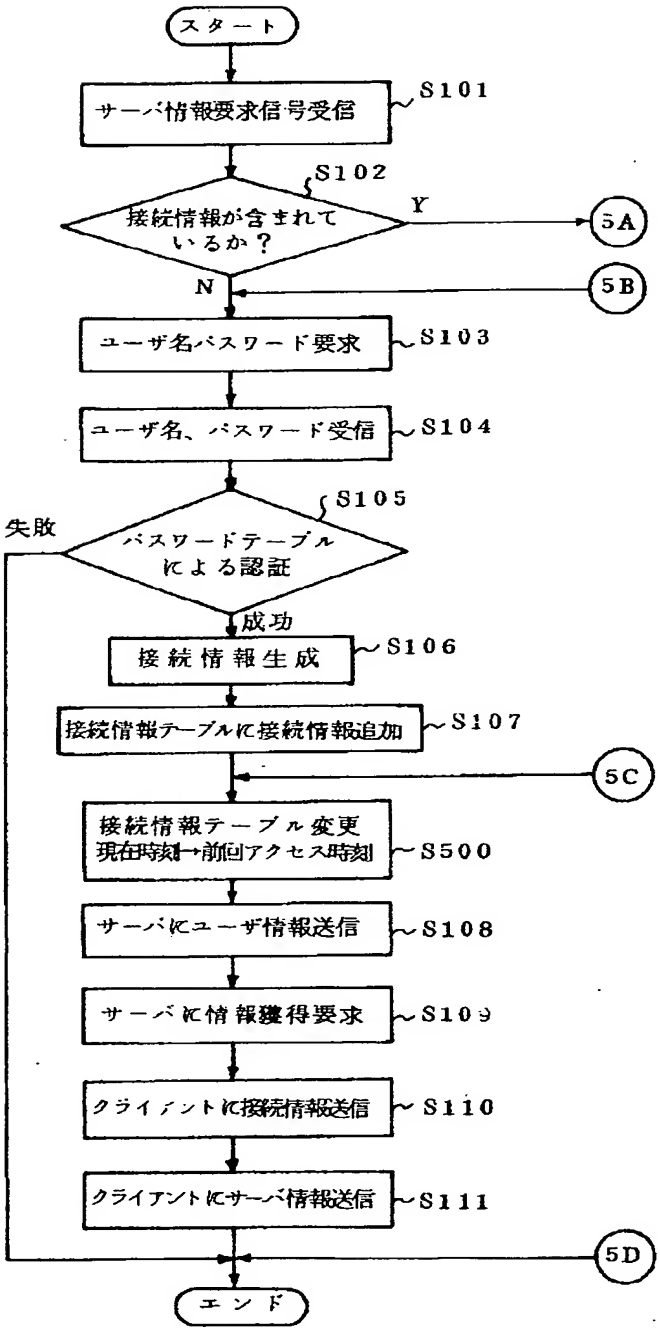
【図13】


24d :パスワードプログラム
ユーザ名 パスワード タイムアウト時間
ユーザA AAAA 3600
ユーザB BBBB 3600
ユーザC CCCC 3600
20d
認証・接続情報生成プログラム
16
クライアントプログラム
14
接続情報
18
サーバプログラム
22
26d:接続情報テーブル
ユーザ名 接続情報 前回アクセス時刻
ユーザA :+1k$% 19970625150020
ユーザB —=0)wd 19970625121035
ユーザC >:*+pq 19970624203515
10:クライアント
12d:サーバ

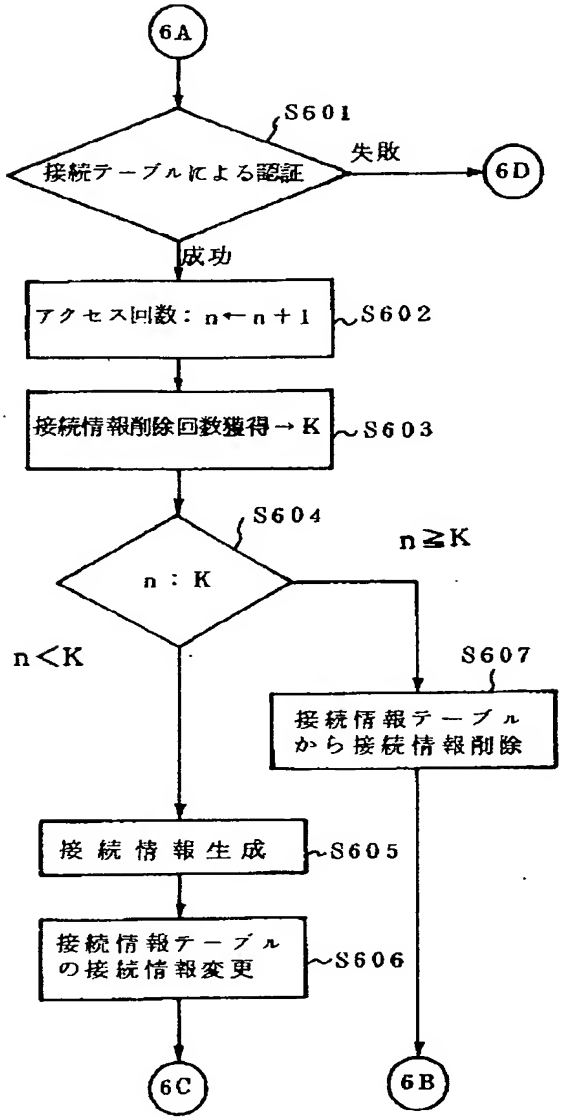
【図16】


24e パスワードプログラム
ユーザ名 パスワード 接続情報削除回数
ユーザA AAAA 20
ユーザB BBBB 20
ユーザC CCCC 20
20e
認証・接続情報生成プログラム
16
クライアントプログラム
14
接続情報
18
サーバプログラム
22
26e 接続情報テーブル
ユーザ名 接続情報 アクセス回数
ユーザA :+1k$% 2
ユーザB —=0)wd 15
ユーザC >:*+pq 6
10:クライアント
12e:サーバ

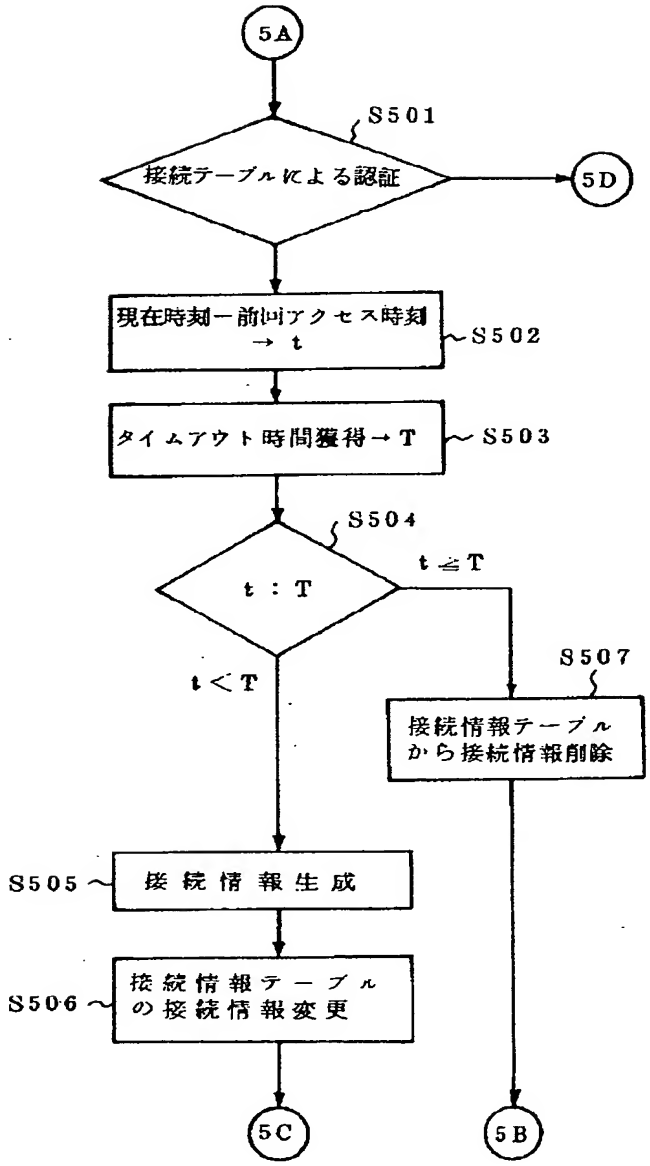
【図１４】


スタート
サーバ情報要求信号受信
S101
S102
接続情報が含まれているか？
Y
5A
N
5B
ユーザ名パスワード要求
S103
ユーザ名、パスワード受信
S104
S105
失敗
パスワードテーブルによる認証
成功
接続情報生成
S106
接続情報テーブルに接続情報追加
S107
5C
接続情報テーブル変更
現在時刻→前回アクセス時刻
S500
サーバにユーザ情報送信
S108
サーバに情報獲得要求
S109
クライアントに接続情報送信
S110
クライアントにサーバ情報送信
S111
5D
エンド

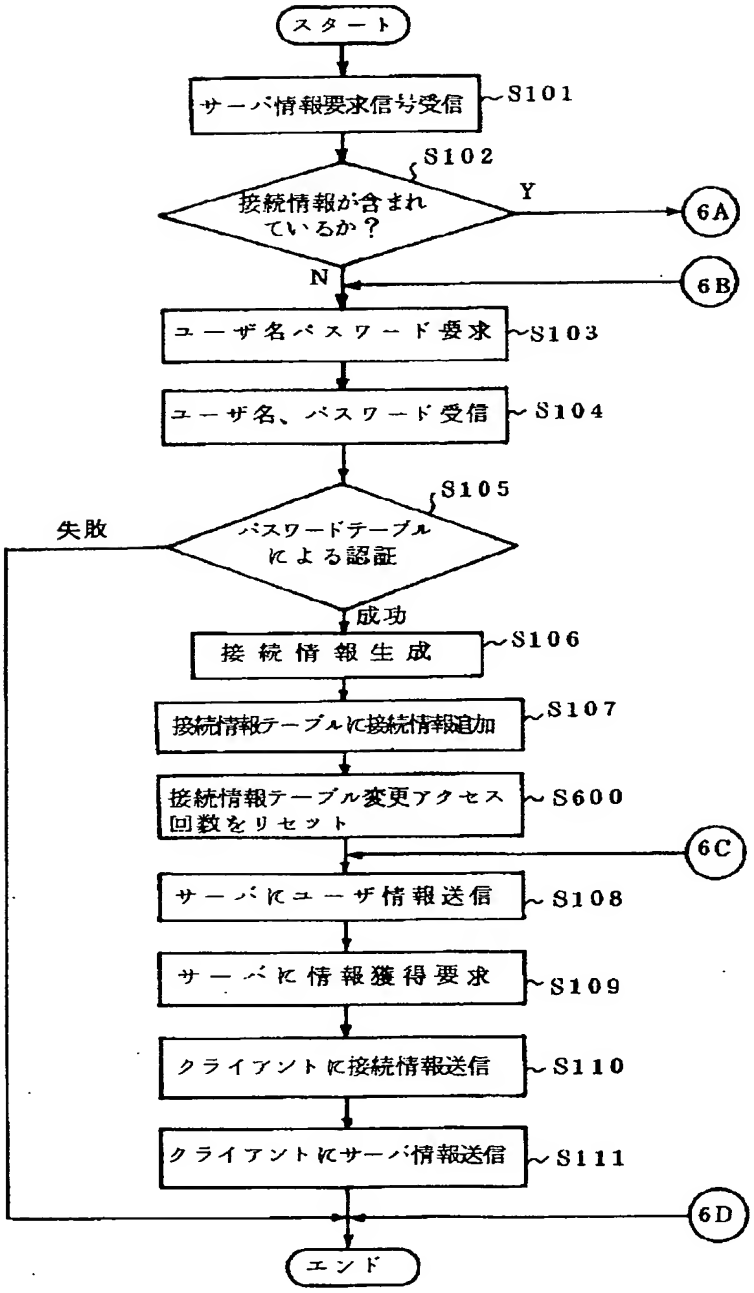
【図１８】


6A
S601
接続テーブルによる認証
失敗
6D
成功
アクセス回数：n←n＋1
S602
接続情報削除回数獲得→K
S603
S604
n：K
n≧K
n＜K
S607
接続情報テーブルから接続情報削除
接続情報生成
S605
接続情報テーブルの接続情報変更
S606
6C
6B

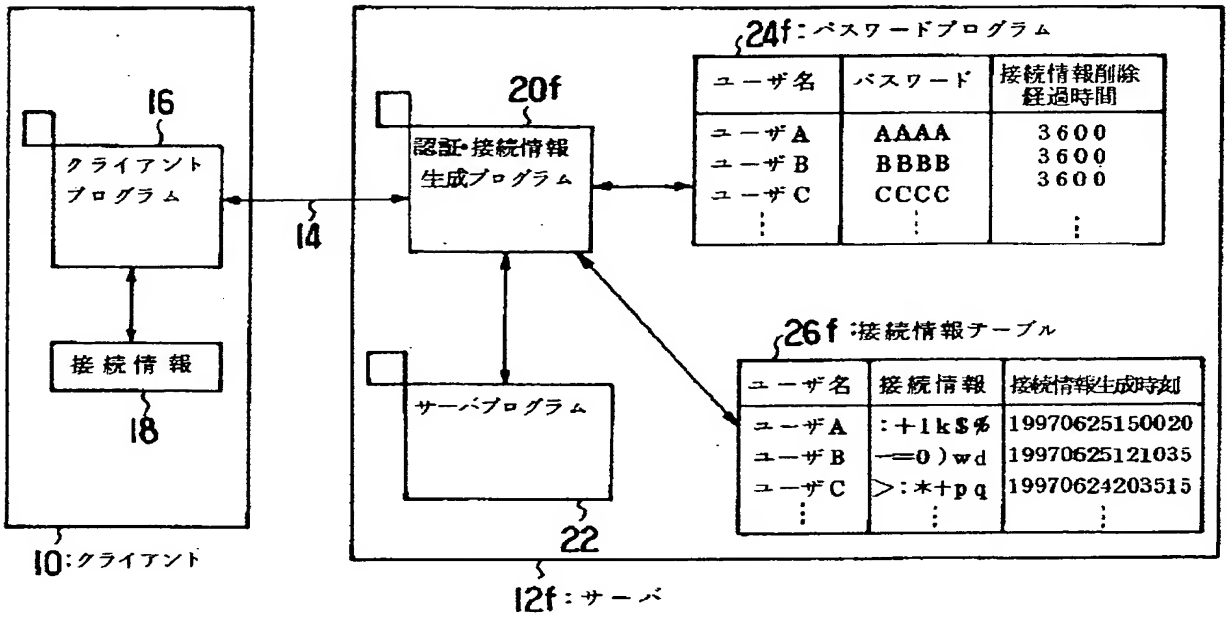
【図１５】


5A
S501
接続テーブルによる認証
5D
現在時刻－前回アクセス時刻 → t
S502
タイムアウト時間獲得→T
S503
S504
t : T
t≧T
t＜T
S507
接続情報テーブルから接続情報削除
S505
接続情報生成
S506
接続情報テーブルの接続情報変更
5C
5B

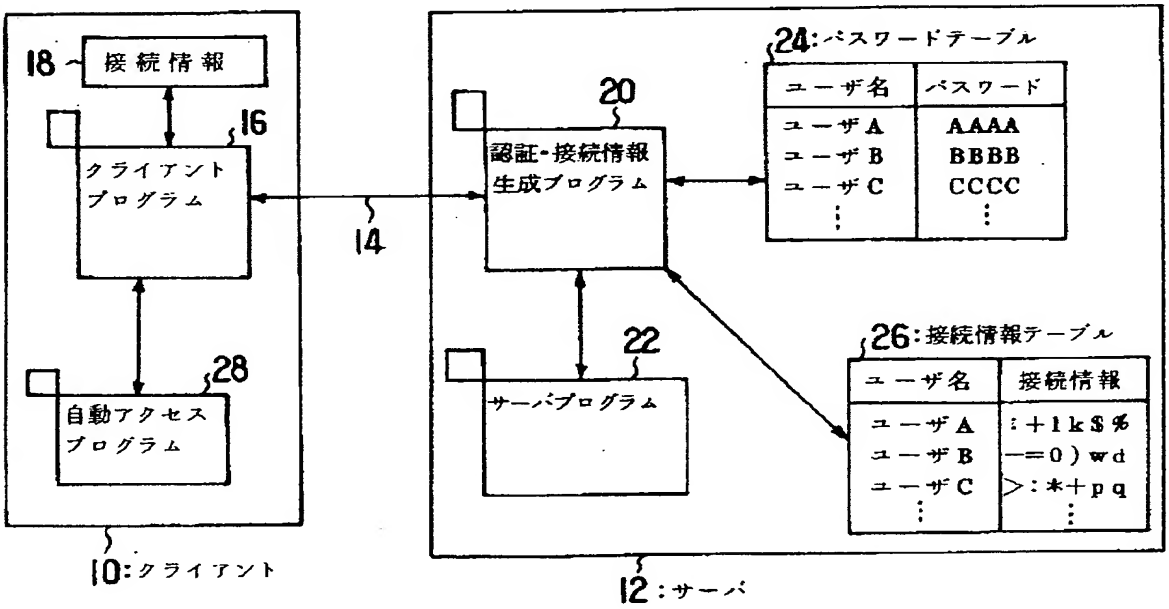
【図１７】


スタート
サーバ情報要求信号受信
S101
S102
接続情報が含まれているか？
Y
6A
N
6B
ユーザ名パスワード要求
S103
ユーザ名、パスワード受信
S104
S105
パスワードテーブルによる認証
失敗
成功
接続情報生成
S106
接続情報テーブルに接続情報追加
S107
接続情報テーブル変更アクセス回数をリセット
S600
6C
サーバにユーザ情報送信
S108
サーバに情報獲得要求
S109
クライアントに接続情報送信
S110
クライアントにサーバ情報送信
S111
6D
エンド

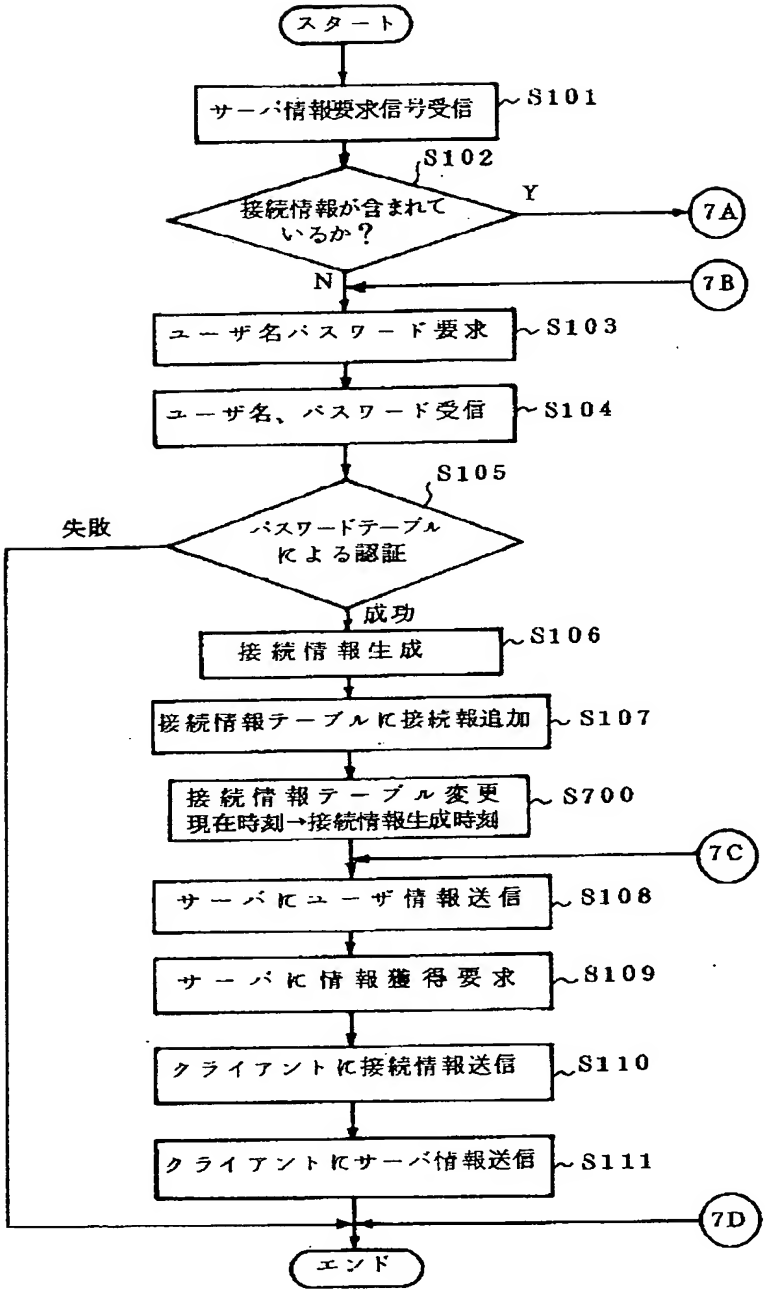
【図１９】


16
クライアント
プログラム
接続情報
18
10:クライアント
14
20f
認証・接続情報
生成プログラム
サーバプログラム
22
12f:サーバ
24f:パスワードプログラム
ユーザ名
パスワード
接続情報削除
経過時間
ユーザA
ユーザB
ユーザC
AAAA
BBBB
CCCC
3600
3600
3600
26f:接続情報テーブル
ユーザ名
接続情報
接続情報生成時刻
ユーザA
ユーザB
ユーザC
:+1k$%
19970625150020
19970625121035
19970624203515

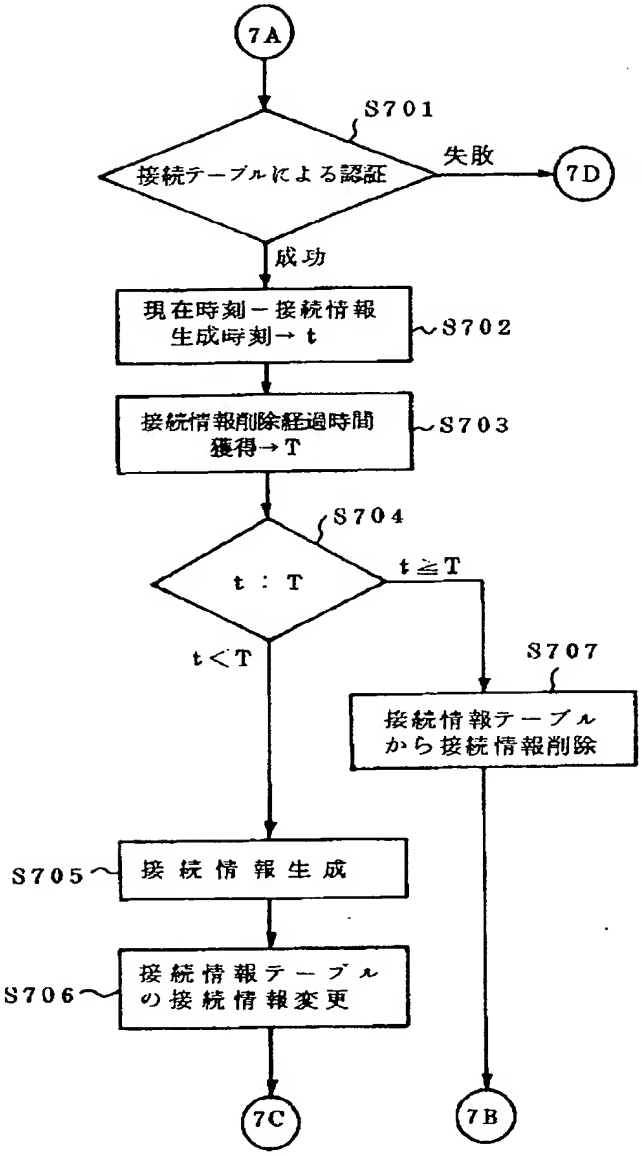
【図２６】


18
接続情報
16
クライアント
プログラム
28
自動アクセス
プログラム
10:クライアント
14
20
認証・接続情報
生成プログラム
サーバプログラム
22
12:サーバ
24:パスワードテーブル
ユーザ名
パスワード
ユーザA
ユーザB
ユーザC
AAAA
BBBB
CCCC
26:接続情報テーブル
ユーザ名
接続情報
ユーザA
ユーザB
ユーザC
:+1k$%

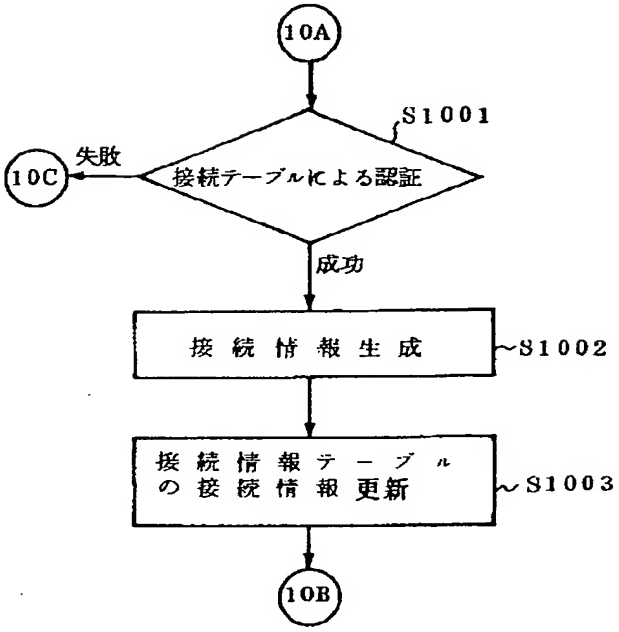
【図20】


スタート
サーバ情報要求信号受信
S101
S102
接続情報が含まれているか？
Y
7A
N
7B
ユーザ名パスワード要求
S103
ユーザ名、パスワード受信
S104
S105
パスワードテーブルによる認証
失敗
成功
接続情報生成
S106
接続情報テーブルに接続報追加
S107
接続情報テーブル変更
現在時刻→接続情報生成時刻
S700
7C
サーバにユーザ情報送信
S108
サーバに情報獲得要求
S109
クライアントに接続情報送信
S110
クライアントにサーバ情報送信
S111
7D
エンド

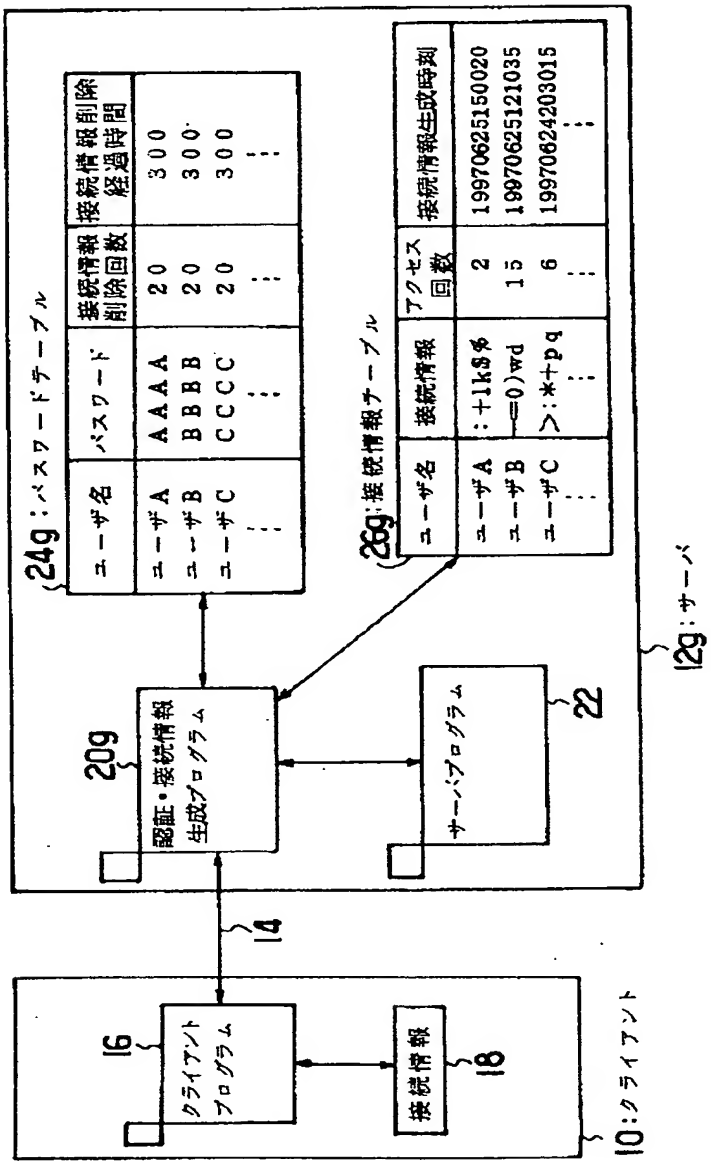
【図２１】


7A
S701
接続テーブルによる認証
失敗
7D
成功
現在時刻－接続情報生成時刻→t
S702
接続情報削除経過時間獲得→T
S703
S704
t：T
t≧T
t<T
S707
接続情報テーブルから接続情報削除
S705
接続情報生成
S706
接続情報テーブルの接続情報変更
7C
7B

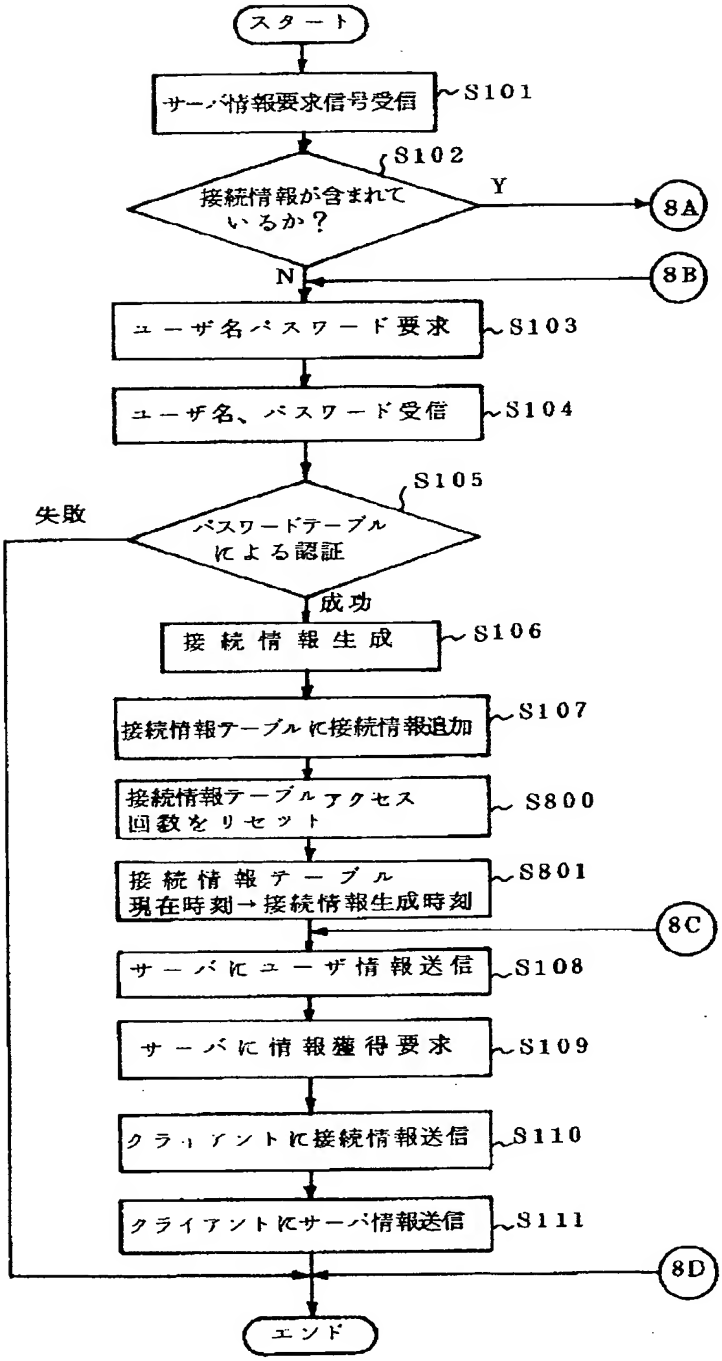
【図２８】


10A
S1001
接続テーブルによる認証
失敗
10C
成功
接続情報生成
S1002
接続情報テーブルの接続情報更新
S1003
10B

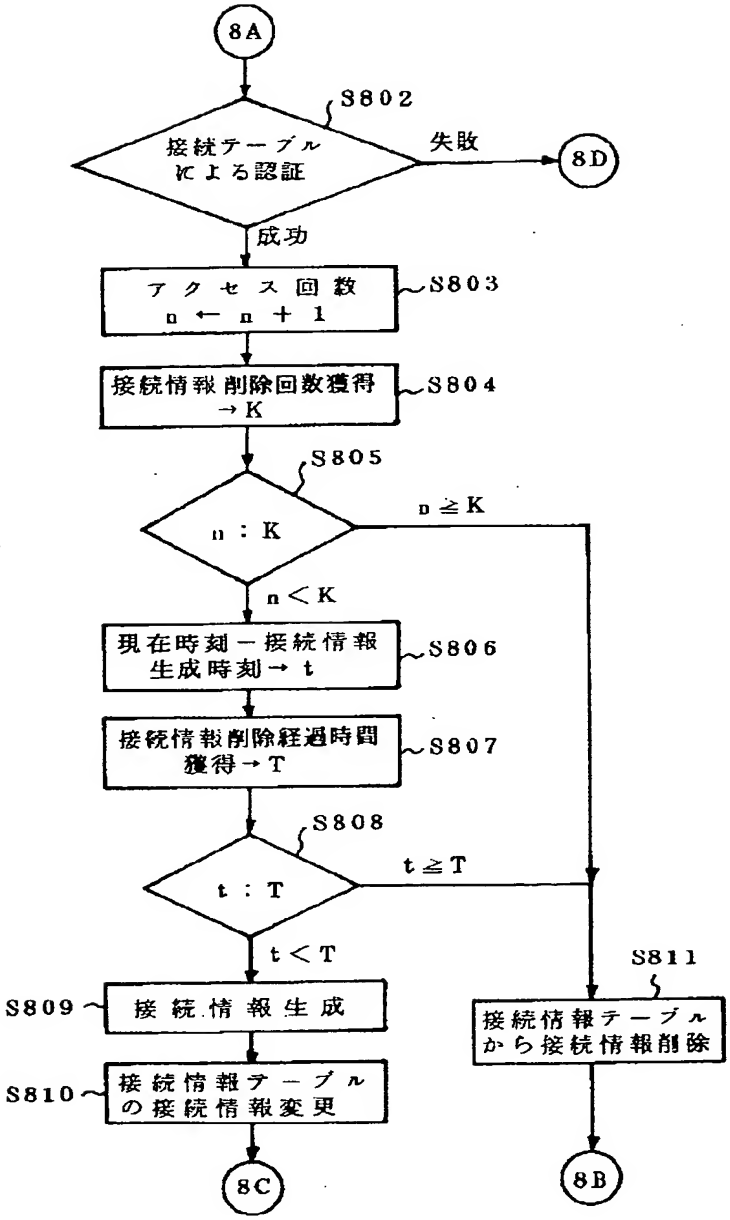
【図２２】


24g：パスワードテーブル
ユーザ名
パスワード
接続情報削除回数
接続情報削除経過時間
ユーザA
ユーザB
ユーザC
AAAA
BBBB
CCCC
20
20
20
300
300
300
26g：接続情報テーブル
ユーザ名
接続情報
アクセス回数
接続情報生成時刻
ユーザA
ユーザB
ユーザC
2
15
6
19970625150020
19970625121035
19970624203015
20g
認証・接続情報生成プログラム
22
サーバプログラム
12g：サーバ
14
16
クライアントプログラム
18
接続情報
10：クライアント

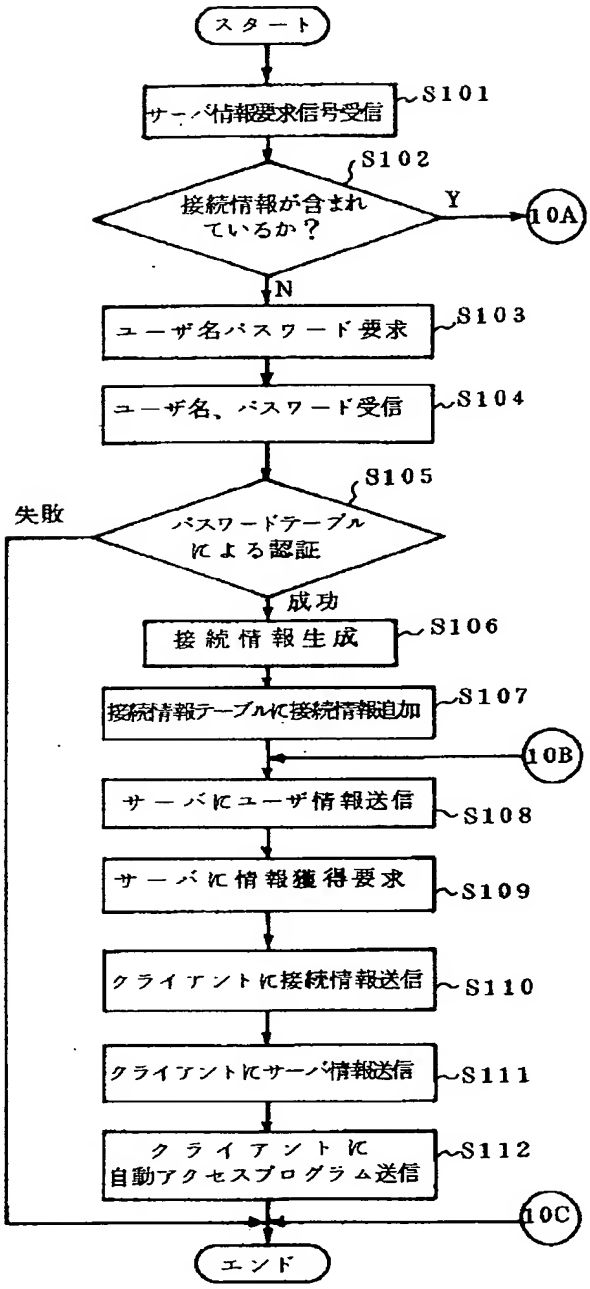
【図２３】


スタート
サーバ情報要求信号受信
S101
S102
接続情報が含まれているか？
Y
8A
N
8B
ユーザ名パスワード要求
S103
ユーザ名、パスワード受信
S104
S105
パスワードテーブルによる認証
失敗
成功
接続情報生成
S106
接続情報テーブルに接続情報追加
S107
接続情報テーブルアクセス回数をリセット
S800
接続情報テーブル現在時刻→接続情報生成時刻
S801
8C
サーバにユーザ情報送信
S108
サーバに情報獲得要求
S109
クライアントに接続情報送信
S110
クライアントにサーバ情報送信
S111
8D
エンド

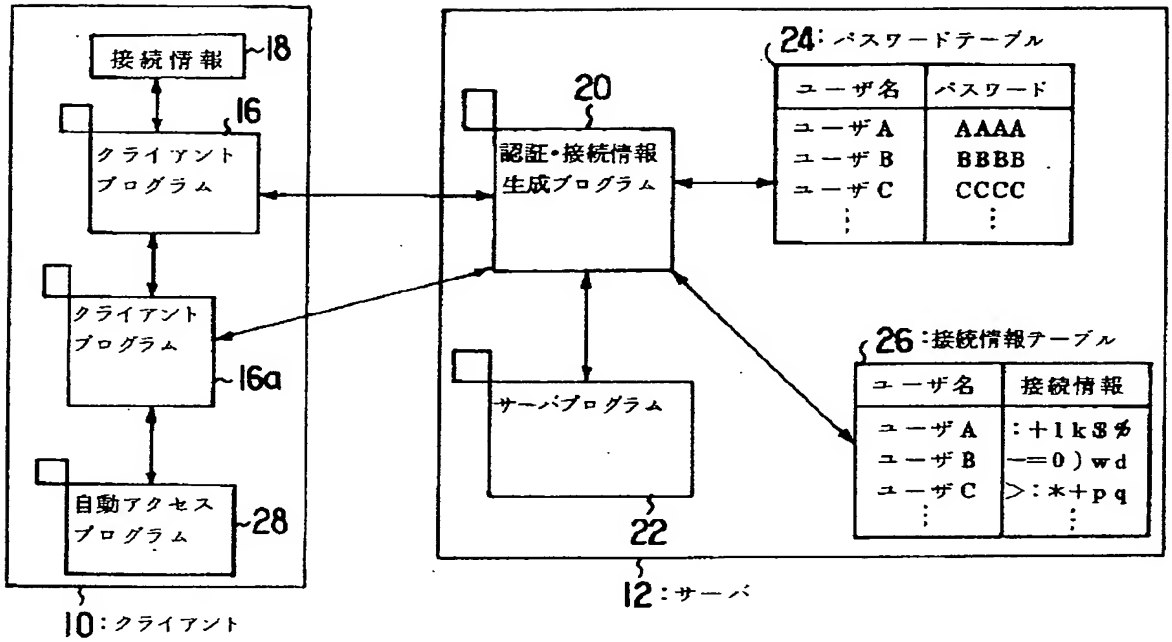
【図２４】


8A
S802
接続テーブルによる認証
失敗
8D
成功
アクセス回数 n ← n + 1
S803
接続情報削除回数獲得 → K
S804
S805
n : K
n ≧ K
n < K
現在時刻－接続情報生成時刻 → t
S806
接続情報削除経過時間獲得 → T
S807
S808
t : T
t ≧ T
t < T
S809
接続情報生成
S810
接続情報テーブルの接続情報変更
8C
S811
接続情報テーブルから接続情報削除
8B

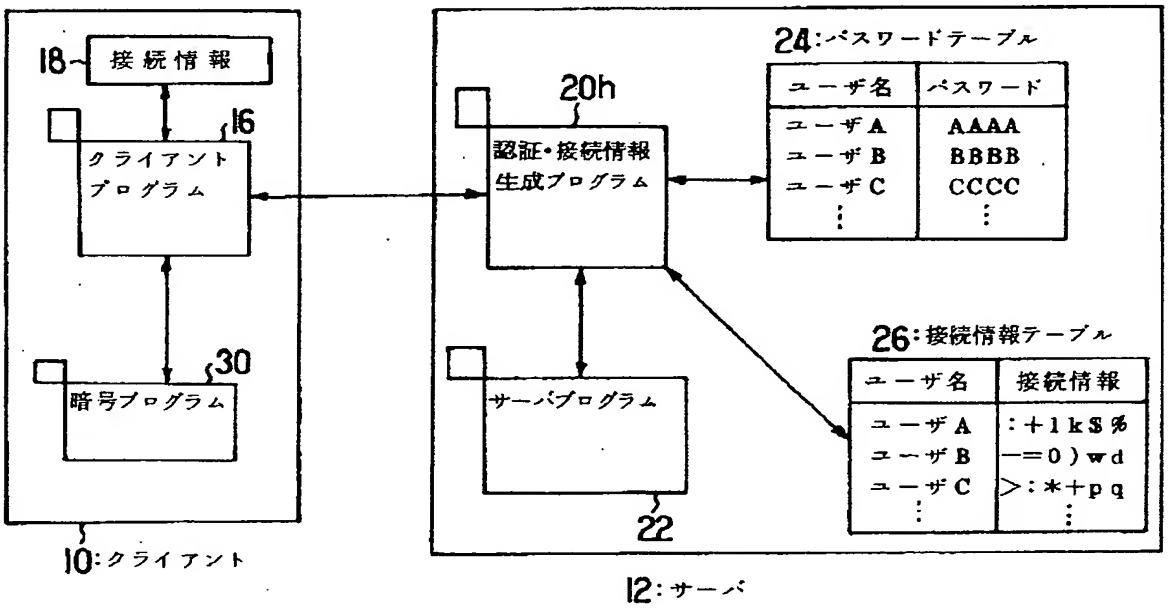
【図２７】


スタート
サーバ情報要求信号受信
S101
S102
接続情報が含まれているか？
Y
10A
N
ユーザ名パスワード要求
S103
ユーザ名、パスワード受信
S104
S105
パスワードテーブルによる認証
失敗
成功
接続情報生成
S106
接続情報テーブルに接続情報追加
S107
10B
サーバにユーザ情報送信
S108
サーバに情報獲得要求
S109
クライアントに接続情報送信
S110
クライアントにサーバ情報送信
S111
クライアントに自動アクセスプログラム送信
S112
10C
エンド

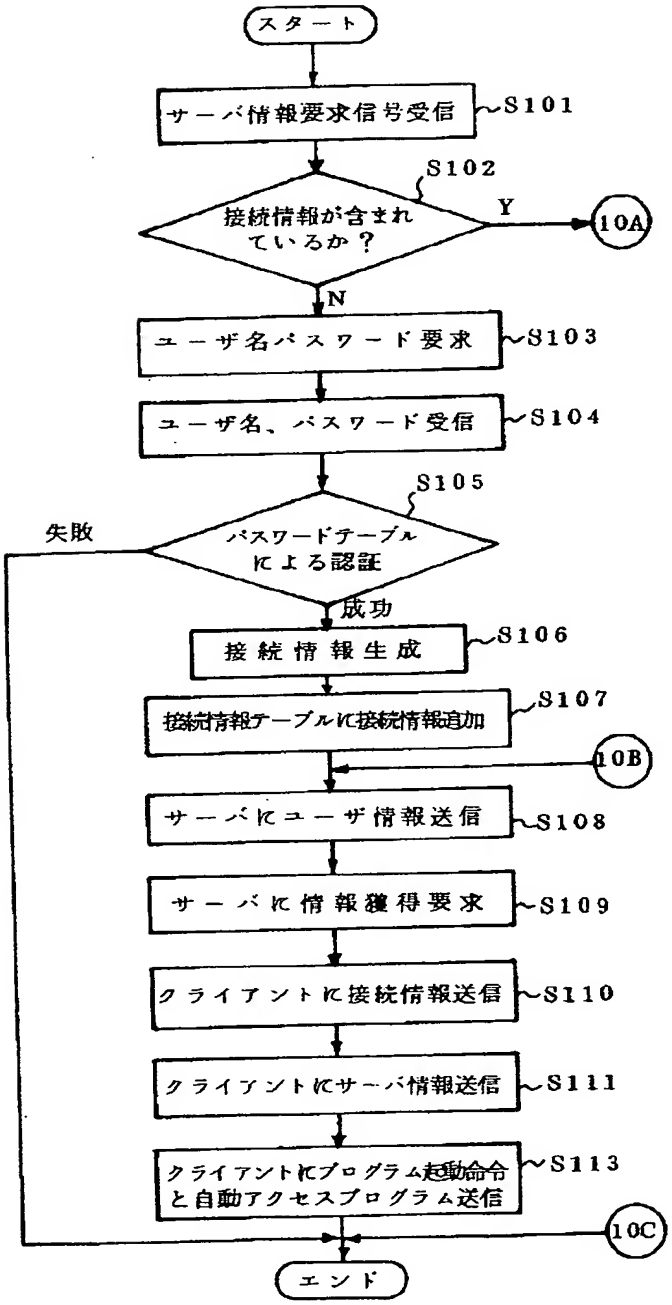
【図29】


接続情報
18
16
クライアント
プログラム
クライアント
プログラム
16a
自動アクセス
プログラム
28
10：クライアント
20
認証・接続情報
生成プログラム
サーバプログラム
22
12：サーバ
24：パスワードテーブル
ユーザ名
パスワード
ユーザA
ユーザB
ユーザC
AAAA
BBBB
CCCC
26：接続情報テーブル
ユーザ名
接続情報
ユーザA
ユーザB
ユーザC

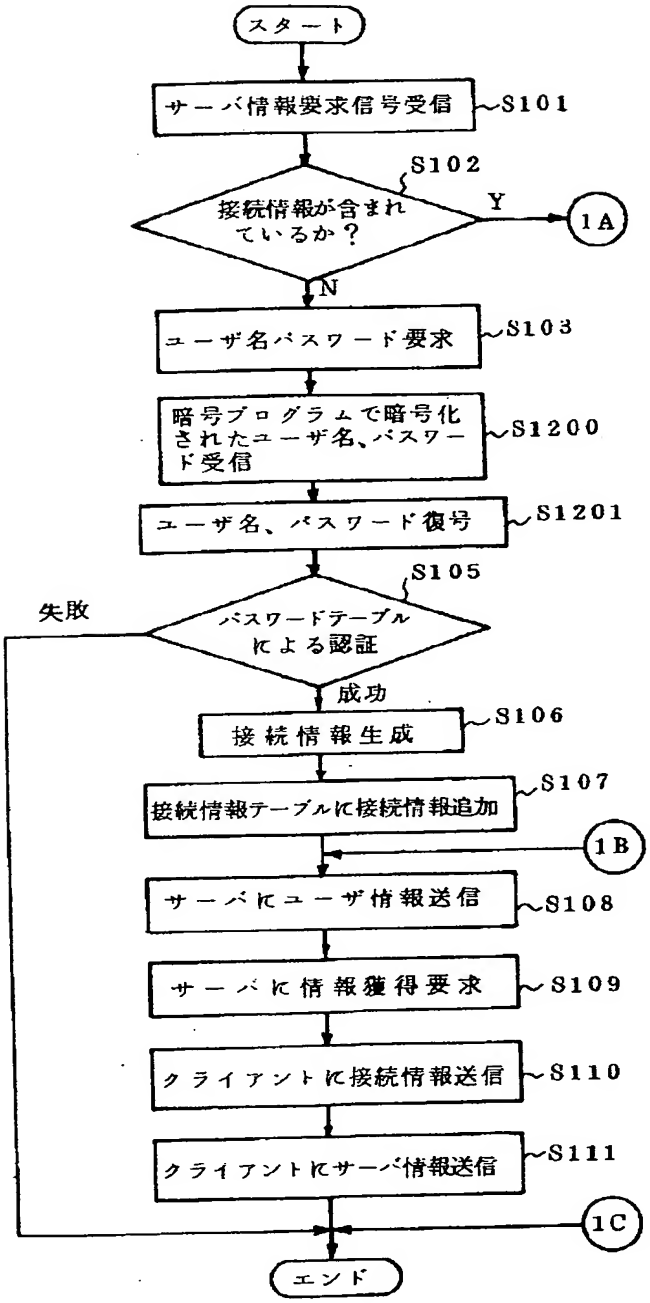
【図31】


18
接続情報
16
クライアント
プログラム
30
暗号プログラム
10：クライアント
20h
認証・接続情報
生成プログラム
サーバプログラム
22
12：サーバ
24：パスワードテーブル
ユーザ名
パスワード
ユーザA
ユーザB
ユーザC
AAAA
BBBB
CCCC
26：接続情報テーブル
ユーザ名
接続情報
ユーザA
ユーザB
ユーザC

【図３０】


スタート
サーバ情報要求信号受信
S101
S102
接続情報が含まれているか？
Y
10A
N
ユーザ名パスワード要求
S103
ユーザ名、パスワード受信
S104
S105
パスワードテーブルによる認証
失敗
成功
接続情報生成
S106
接続情報テーブルに接続情報追加
S107
10B
サーバにユーザ情報送信
S108
サーバに情報獲得要求
S109
クライアントに接続情報送信
S110
クライアントにサーバ情報送信
S111
クライアントにプログラム起動命令と自動アクセスプログラム送信
S113
10C
エンド

【図３２】


スタート
サーバ情報要求信号受信
S101
S102
接続情報が含まれているか？
Y
1A
N
ユーザ名パスワード要求
S103
暗号プログラムで暗号化されたユーザ名、パスワード受信
S1200
ユーザ名、パスワード復号
S1201
S105
失敗
パスワードテーブルによる認証
成功
接続情報生成
S106
接続情報テーブルに接続情報追加
S107
1B
サーバにユーザ情報送信
S108
サーバに情報獲得要求
S109
クライアントに接続情報送信
S110
クライアントにサーバ情報送信
S111
1C
エンド

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-167551
(43)Date of publication of application : 22.06.1999

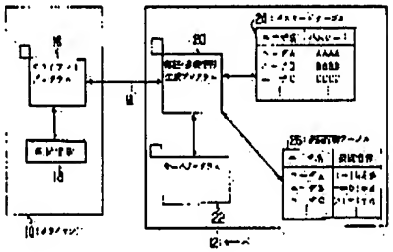
(51)Int.Cl. G06F 15/00
H04L 9/32

(21)Application number : 09-332889
(22)Date of filing : 03.12.1997

(71)Applicant : MITSUBISHI ELECTRIC CORP
(72)Inventor : SHIRAKI HIROAKI
KAMASAKA HITOSHI
KOWATARI MASASHI

(54) SERVER AND ITS ACCESS CONTROL METHOD AND INFORMATION RECORD MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To reduce the possibility of leakage of the authentication information when the access control is performed between the client servers.
SOLUTION: When the access control is performed between a client 10 kept in a connection-less environment and a server 12, the server 12 generates and sends the connection information to the client 10 that succeeded to authenticate its user via a password table 24. At the same time, the connection information is stored in a connection information table 26 of the server 12. Receiving the connection information corresponding to a request signal from the client 10, the server 12 authenticates the user of the client 10 based on the said connection information and the connection information stored in the table 26. When the user can be authenticated, the server information corresponding to the request signal corresponding to the connection information is acquired from a server program 22 and sent back to the client 10.



LEGAL STATUS

[Date of request for examination] 03.12.1997
[Date of sending the examiner's decision of rejection] 30.09.2003
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

Searching PAJ http://www19.ipdl.ncipi.go.jp/PA1/result/detail/mai...

* NOTICES *

JPO and NCIPI are not responsible for any damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1] In the server which answers the client in the server information corresponding to the demand signal transmitted from a client An initial entry transmitting means to generate an initial entry to the client which succeeded in user authentication with a password, and to transmit to it, A connection information storage means to memorize the initial entry transmitted to a client with said initial entry transmitting means, An authentication means to perform user authentication of a client based on the initial entry and the initial entry memorized by said connection information storage means when the initial entry matched with the demand signal from the client is received, The server characterized by including a server information reply means to answer a client in the server information corresponding to the demand signal matched with the initial entry when it succeeds in the user authentication of a client with said authentication means.
[Claim 2] The server according to claim 1 characterized by including further the 1st renewal means of an initial entry which memorizes the new initial entry for said connection information storage means while generating a new initial entry and transmitting to a client, when the same initial entry is received more than the count of predetermined from a client.
[Claim 3] The server according to claim 1 or 2 characterized by including further the 2nd renewal means of an initial entry which memorizes the new initial entry for said connection information storage means while generating a new initial entry and transmitting to a client, when predetermined time has passed since generation of the initial entry by said initial entry transmitting means.
[Claim 4] The server according to claim 1 to 3 characterized by including further the 1st authentication termination means which once stops the user authentication of the client by said authentication means when there is no access from the again same client, even if predetermined time passes since the event of the last access.
[Claim 5] The server according to claim 1 to 4 characterized by including further the 2nd authentication termination means which once stops the user authentication of the client by said authentication means when there is access from the client after the user authentication of a client with a password more than the count of predetermined.
[Claim 6] The server according to claim 1 to 5 characterized by including further the 3rd authentication termination means which once stops the user authentication of the client by said authentication means when predetermined time passes after the user authentication of a client with a password.
[Claim 7] The server according to claim 1 to 6 characterized by including further the 4th authentication termination means which stops the user authentication of the client by said authentication means when the predetermined demand signal of the purport which should cancel an initial entry from a client is received.
[Claim 8] The server according to claim 1 to 7 characterized by including further a client-server access generating means to generate access to a server from the client for every fixed time amount using an initial entry.
[Claim 9] Said client-server access generating means is a server according to claim 8 characterized by including an activation module transmitting means to transmit the activation module which controls a client, to a client so that access to the server using an initial entry may be performed for every fixed time amount.
[Claim 10] It is the server according to claim 8 characterized by for said server information being hypertext information and said client-server access generating means including the tag information on a purport that access to the server which used the initial entry should be performed after predetermined time in said server information.
[Claim 11] The server according to claim 1 to 9 characterized by having further a decryption means to decrypt this password when the password enciphered from the client is transmitted.
[Claim 12] It is the access-control approach of the server which answers the client in the server information corresponding to the demand signal transmitted from a client. The initial entry transmitting step which generates an initial entry to the client which succeeded in user authentication with a password, and is transmitted to it, The connection information storage step which memorizes the initial entry transmitted to a client at said initial entry transmitting step, The authentication step which performs user authentication of a client based on the initial entry and the initial entry memorized at said connection information storage step when the initial entry matched with the demand signal from the client is received, The

JP,11-167551,A [CLAIMS] http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejj...

access-control approach of the server characterized by including the server information reply step which answers a client in the server information corresponding to the demand signal matched with the initial entry when it succeeds in the user authentication of a client at said authentication step.
[Claim 13] The server information corresponding to the demand signal to which a computer is transmitted from a client The initial entry transmitting step which is the information record medium which recorded the program for making it operate as a server which answers the client, generates an initial entry to the client which succeeded in user authentication with a password, and is transmitted to it, The connection information storage step which memorizes the initial entry transmitted to a client at said initial entry transmitting step, The authentication step which performs user authentication of a client based on the initial entry and the initial entry memorized at said connection information storage step when the initial entry matched with the demand signal from the client is received, The server information reply step which answers a client in the server information corresponding to the demand signal matched with the initial entry when it succeeds in the user authentication of a client at said authentication step, The information record medium characterized by recording the program for performing a computer.

[Translation done.]

* NOTICES *

JPO and NCIPI are not responsible for any damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] Especially this invention relates to the access-control technique over the client of a server about the access-control approach of a server and a server, and an information record medium.
[0002]
[Description of the Prior Art] In the connectionless environment where the client is answered, communication link connection is not maintained between client-server in the server information to which a server corresponds to the demand signal from a client. Therefore, if a client program tends to acquire the information on the server by which the access control is carried out, even if it is the case where it has already succeeded in user authentication, the authentication by the input of a user name or a password whenever a client transmits a demand signal to a server is needed. For this reason, when a demand signal was transmitted to a server, the user had to enter the user name and the password in the client, had to transmit them to the server, and had the problem that actuation became complicated.
[0003] On the other hand, once it memorizes the user name and the password in the memory on the machine of a client and succeeds in user authentication with a user name and a password in access to a certain server, by access to the same subsequent server, avoiding this problem will also be considered by transmitting the user name and password on memory automatically each time.
[0004]
[Problem(s) to be Solved by the Invention] However, in the access control between client-server, authentication information, such as a user name and a password, being transmitted by simple text data in many cases, and transmitting a password at every access to a server from a client as

mentioned above has the problem of being easy to cause unlawful access to the increase of the danger of tapping, and a user depended for becoming completely.
[0005] On the other hand, in the security method concerning JP,4-182768,A, secret enquiry information is changed at every access in the communication environment which establishes a connection. That is, in this method, user authentication of a client is performed by using the password information of immobilization, and the secret enquiry information which changes each time by the pair for connection establishment with a host computer. However, since transmission and reception of a password are frequently performed between a client and a host computer also in this technique, the danger of tapping of such information is high. Since secret enquiry information is furthermore saved at a client, there is a problem that a host computer can be accessed only from the client.
[0006] This invention is made in view of the above-mentioned technical problem, and the object is in offering the information record medium which recorded the program which realizes the access-control approach of a server and a server and it which can lessen possibility of leakage of authentication information in the access control between client-server.
[0007]
[Means for Solving the Problem] In the server which answers the client in the server information corresponding to the demand signal with which the 1st invention is transmitted from a client in order to solve the above-mentioned technical problem An initial entry transmitting means to generate an initial entry to the client which succeeded in user authentication with a password, and to transmit to it, A connection information storage means to memorize the initial entry transmitted to a client with said initial entry transmitting means, An authentication means to perform user authentication of a client based on the initial entry and the initial entry memorized by said connection information storage means when the initial entry matched with the demand signal from the client is received, When it succeeds in the user authentication of a client with said authentication means, a server information reply means to answer a client in the server information corresponding to the demand signal matched with the initial entry is included.

[0008] In the 1st invention, the 2nd invention includes further the 1st renewal means of an initial entry which memorizes the new initial entry for said connection information storage means while it generates a new initial entry and transmits to a client, when the same initial entry is received more than the count of predetermined from a client.
[0009] In the 1st or 2nd invention, the 3rd invention includes further the 2nd renewal means of an initial entry which memorizes the new initial entry for

said connection information storage means while it generates a new initial entry and transmits to a client, when predetermined time has passed since generation of the initial entry by said initial entry transmitting means.

[0010] In the 1st thru/or the 3rd one of invention, the 4th invention includes further the 1st authentication termination means which once stops the user authentication of the client by said authentication means, when there is no access from the again same client, even if predetermined time passes since the event of the last access.

[0011] In the 1st thru/or the 4th one of invention, after the user authentication of a client with a password, the 5th invention includes further the 2nd authentication termination means which once stops the user authentication of the client by said authentication means, when there is access from the client more than the count of predetermined.

[0012] In the 1st thru/or the 5th one of invention, after the user authentication of a client with a password, the 6th invention includes further the 3rd authentication termination means which once stops the user authentication of the client by said authentication means, when predetermined time passes.

[0013] In the 1st thru/or the 6th one of invention, the 7th invention includes further the 4th authentication termination means which stops the user authentication of the client by said authentication means, when the predetermined demand signal of the purport which should cancel an initial entry from a client is received.

[0014] The 8th invention includes further a client-server access generating means to generate access to a server from the client for every fixed time amount using an initial entry, in the 1st thru/or the 7th one of invention.

[0015] In the 8th invention, the 9th invention includes an activation module transmitting means to transmit the activation module which controls a client so that said client-server access generating means may perform access to the server using an initial entry for every fixed time amount to a client.

[0016] In the 8th invention, said server information of the 10th invention is hypertext information, and said client-server access generating means includes the tag information on a purport that access to the server which used the initial entry should be performed after predetermined time in said server information.

[0017] In the 1st thru/or the 9th one of invention, the 11th invention is further equipped with a decryption means to decrypt this password, when the password enciphered from the client is transmitted.

[0018] The 12th invention the server information corresponding to the demand signal transmitted from a client The initial entry transmitting step which is the access-control approach of the server which answers the client, generates an initial entry to the client which succeeded in user

authentication with a password, and is transmitted to it, The connection information storage step which memorizes the initial entry transmitted to a client at said initial entry transmitting step, The authentication step which performs user authentication of a client based on the initial entry and the initial entry memorized at said connection information storage step when the initial entry matched with the demand signal from the client is received, When it succeeds in the user authentication of a client at said authentication step, the server information reply step which answers a client in the server information corresponding to the demand signal matched with the initial entry is included.

[0019] The 13th invention the server information corresponding to the demand signal to which a computer is transmitted from a client The initial entry transmitting step which is the information record medium which recorded the program for making it operate as a server which answers the client, generates an initial entry to the client which succeeded in user authentication with a password, and is transmitted to it, The connection information storage step which memorizes the initial entry transmitted to a client at said initial entry transmitting step, The authentication step which performs user authentication of a client based on the initial entry and the initial entry memorized at said connection information storage step when the initial entry matched with the demand signal from the client is received, When it succeeds in the user authentication of a client at said authentication step, the program for making a computer perform the server information reply step which answers a client in the server information corresponding to the demand signal matched with the initial entry is recorded.

[0020]

[Embodiment of the Invention] Hereafter, the gestalt of operation of this invention is explained to a detail based on a drawing.

[0021] Gestalt 1. drawing 1 of operation is the functional block diagram showing the communication system concerning the gestalt 1 of operation of this invention. Below, it clarifies about one of the operation gestalten of the information record medium which recorded the program for realizing the access-control approach of the server concerning this invention, a client, and a server, and it through disclosure of this communication system.

[0022] As shown in this drawing, a client 10 and a server 12 are mutually connected by the means of communications 14, such as the Internet, possible [a communication link], and this communication system becomes. And in this communication system, communication link connection of a client 10 and the server 12 is made in the connectionless environment, and a client 10 transmits the demand signal of the purport which requires server information from a server 12. On the other hand, a server 12 answers the client 10 in the server information corresponding to the demand signal

received from a client 10. This configuration is common in a WWW (World Wide Web) system etc., the above-mentioned demand signal is equivalent to URL (Uniform Resource Locator) in this case, and the above-mentioned server information is equivalent to hypertext information.

[0023] A client 10 is constituted by information processors, such as PC, and contains the client program 16 which is loaded to main storage and performed by CPU. And the initial entry is especially memorized by the storage means 18, such as memory. If server information is received from a server 12 to the demand signal while this client program 16 transmits a demand signal to a server 12 through means of communications 14, it will perform the display display based on the server information with the indicating equipment which is not illustrated. Moreover, a client program 16 transmits the initial entry to a server 12 with a demand signal, when the initial entry is memorized by the storage means 18.

[0024] The server 12 includes the authentication and the initial entry generator 20 which is constituted by information processors, such as PC, is loaded to main storage like a client 10, and is performed by CPU, and the server program 22. And the password table 24 and the initial entry table 26 are memorized by especially the external storage.

[0025] First, authentication and the initial entry generator 20 perform user authentication of a client 10 based on the information and password table 24, when a user name and a password are transmitted from a client program 16. And when it succeeds in the user authentication of a client 10, while generating the initial entry over the client 10 and transmitting to a client 10, this information is matched with a user name and it memorizes on the initial entry table 26.

[0026] Moreover, authentication and the initial entry generator 20 perform user authentication of a client 10 based on the initial entry and initial entry table 26, when an initial entry is transmitted with a demand signal from a client program 16. And when it succeeds in the user authentication of a client 10, transmission of the server information which a client 10 requires from the server program 22 is required of the server program 22, and the server information received from the server program 22 is transmitted to a client 10.

[0027] Here, the server program 22 is a program which answers a letter in server information, when a demand signal is received. Moreover, the user name (ID) of the user who is planning that a server 12 is accessed, and the password and ** which were given to the user are matched with the password table 24, and it memorizes. Furthermore, the initial entry table 26 is a table on which the initial entry generated by authentication and the initial entry generator 20 is memorized, and the initial entry and ** which were generated to the user name and user name of the client 10 which accessed

the server 12 are matched, and it is memorized.

[0028] In addition, in the server 12 contained in the above communication system, authentication and the initial entry generator 20 function as an initial entry transmitting means to generate an initial entry to the client 10 which succeeded in user authentication with a password, and to transmit to it. Moreover, the initial entry table 26 functions as a connection information storage means to memorize the initial entry transmitted to a client 10 with an initial entry transmitting means. Furthermore, authentication and the initial entry generator 20 When the initial entry matched with the demand signal from the client 10 is received, while functioning as an authentication means to perform user authentication of a client 10, based on the initial entry and the initial entry memorized by the connection information storage means When it succeeds in the user authentication of a client 10 with an authentication means, it functions as a server information reply means to transmit the server information corresponding to the demand signal matched with the initial entry to a client 10.

[0029] Hereafter, actuation of this communication system which has this configuration is explained based on flow drawing shown in drawing 2 and drawing 3 .

[0030] As shown in drawing 2 , by the server 12, authentication and the initial entry generator 20 receive the demand signal from a client 10 first (S101). And it judges whether the initial entry is included in the received demand signal (S102), and if the initial entry is not included, a user name and a password are required from a client 10 (S103). On the other hand, if a user name and a password are received from a client 10 (S104), authentication and the initial entry generator 20 will perform user authentication of a client 10 based on the user name and password which were received, and password table 24 next. And if the user authentication of the client 10 on the password table 24 goes wrong (S105), the communications processing between a client 10 and a server 12 will be ended.

[0031] Moreover, if authentication and the initial entry generator 20 succeed in the user authentication of the client 10 on the password table 24 in S105, an initial entry will be generated (S106) and additional record of the initial entry will be carried out with a user name at the initial entry table 26 (S107). This initial entry is enciphered and generated by the random combination of a figure, a notation, and an alphabetic character. Next, authentication and the initial entry generator 20 transmit the demand signal for acquiring server information while transmitting User Information, such as a user name, to the server program 22 (S108) (S109). User Information transmitted to the server program 22 can be used if required of the server program 22 concerned. And authentication and the initial entry generator 20 transmit the server information received from the server program 22 to a client 10 while

transmitting the initial entry generated by S106 to a client 10 (S110) (S111).
[0032] When it is judged that the initial entry is included in the demand signal which authentication and the initial entry generator 20 receive from a client 10 in S102 on the other hand, user authentication of a client 10 is performed by investigating whether next the initial entry of this authentication and initial entry generator 20 is the same as that of what is already recorded on the initial entry table 26 (S112). And if it succeeds in the user authentication of a client 10 (S113), processing will be moved to S108 and processing for answering a letter in server information to a client 10 will be performed. Moreover, if the user authentication of a client 10 goes wrong in S113, the communication link between a client 10 and a server 12 will be ended.
[0033] Since the count to which an exchange of a password is performed between a client 10 and a server 12 can be lessened according to the gestalt of the operation explained above, unlawful access by leakage of a password can be prevented. Moreover, if an initial entry can be changed frequently, it can be made to function as a dynamic password so to speak and it carries out like this, leakage of the initial entry situation can also be prevented and unlawful access can be prevented still more certainly.
[0034] Gestalt 2. drawing 4 of operation is the functional block diagram showing the communication system concerning the gestalt 2 of operation of this invention. The communication system shown in this drawing is looked like [the content of password table 24a and initial entry table 26a, and processing of authentication and initial entry generator 20a], and has the description. And since the server program 22 of a client 10 and its internal configuration, and server 12a is the same as that of the communication system concerning the gestalt 1 of operation, it attaches the same sign here and omits explanation.
[0035] First, it matches with a user name and a password and each user's count of connection change information is memorized by password table 24a of the communication system concerning the gestalt of this operation. This count of connection change information is the set point which determines the updating conditions of the initial entry memorized by initial entry table 26a, and a setting-out input is beforehand done by the user of a client 10 or a server 12 with the input means which is not illustrated.
[0036] Moreover, it matches with a user name and an initial entry, and each user's count of access is memorized by initial entry table 26a of the communication system concerning the gestalt of this operation. After an initial entry is generated and this count of access is stored in initial entry table 26a, it expresses the next count of access of that client 10.
[0037] On the other hand, whenever authentication and initial entry generator 20a of this communication system have access of a client 10, it increments and updates the column of the count of access of the initial

entry table 26. And if the value of the count of connection change information the count of access is remembered to be by password table 24a is reached, while generating a new initial entry and transmitting to a client 10, the value of the initial entry already recorded on initial entry table 26a is updated to a new thing. Moreover, the value of the count of access is reset to 0 at this time.
[0038] That is, in the gestalt of this operation, when authentication and initial entry generator 20a receive the same initial entry more than the count of predetermined from a client, while generating a new initial entry and transmitting to a client 10, it functions also as 1st renewal means of an initial entry which memorizes the new initial entry to initial entry table 26a.
[0039] Hereafter, actuation of this communication system which has this configuration is explained based on flow drawing shown in drawing 5 and drawing 6 . Since flow drawing shown in drawing 5 adds the processing flow S200 which resets the count of access of initial entry table 26a to 0 between S107 and S108 in flow drawing shown in drawing 2 , it attaches the same sign as drawing 2 about other processings, and stops it to easy explanation here.
[0040] First, in flow drawing shown in drawing 5 , authentication and initial entry generator 20a receive a demand signal from a client 10 (S101), and when the initial entry is included in the demand signal, as shown in (S102) and drawing 6 , user authentication of a client 10 is performed based on the initial entry and initial entry table 26 (S201). And if the user authentication of the client 10 using an initial entry goes wrong, the communication link between a client 10 and a server 12 will be ended.
[0041] On the other hand, if it succeeds in the user authentication of the client 10 using an initial entry, authentication and the initial entry generator 20 will increment the value of the count of access memorized by initial entry table 26a next, and will update the value n of the count of access of initial entry table 26a (S202). Furthermore, authentication and the initial entry generator 20 read the value K of the count of connection change information from password table 24a (S203), and compares the value and value of the count of access (S204). And if it is a value with the value n of the count of access smaller than the value K which is a count of connection change information, processing will be moved to S108 (drawing 5), it will usually pass, and access processing to the server program 22 will be performed (S108). On the other hand, if it is beyond the value K whose value n of the count of access is a count of connection change information, authentication and the initial entry generator 20 will generate a new initial entry (S205), will store it in the initial entry table 26, and will update an initial entry (S206). Furthermore, authentication and the initial entry generator 20 reset the value n of the count of access of the initial entry table 26 to 0 (S200, drawing 5). Then, it usually passes and access processing to the server program 22 is

performed (S108). Under the present circumstances, the initial entry transmitted to a client 10 in S110 is newly generated in S205. A client program 16 receives this new initial entry from a server 12, and updates the old initial entry already memorized by the storage means 18.

[0042] According to the gestalt of the operation explained above, an initial entry is updated when the count of access becomes more than the count of fixed. While being able to lessen by this possibility that an initial entry will be intercepted, also when an initial entry is intercepted, unlawful access which used the initial entry and which is depended for becoming completely can be restricted.

[0043] Gestalt 3. drawing 7 of operation is the functional block diagram showing the communication system concerning the gestalt 3 of operation of this invention. As compared with the communication system concerning the gestalt 1 of operation, or 2, the communication system shown in this drawing is looked like [the content of password table 24b and initial entry table 26b, and processing of authentication and initial entry generator 20b], and has the description. And since the server program 22 of the configuration of a client 10 and server 12b is the same as that of the communication system concerning the gestalt 1 of operation, or 2, it attaches the same sign here and omits explanation.

[0044] First, it matches with a user name and a password and each user's connection change information elapsed time is memorized by password table 24b of the communication system concerning the gestalt of this operation. This connection change information elapsed time is the set point which determines the updating conditions of the initial entry memorized by initial entry table 26b, and a setting-out input is beforehand done by the user of a client 10 or server 12b with the input means which is not illustrated.

[0045] Moreover, it matches with a user name and an initial entry, and each user's initial entry generation time of day is memorized by initial entry table 26b of the communication system concerning the gestalt of this operation. This initial entry generation time of day expresses the time of day when the initial entry was generated.

[0046] On the other hand, whenever authentication and initial entry generator 20b of this communication system have access of a client 10, it calculates the elapsed time from the initial entry generation time of day of initial entry table 26b. And if the value of the connection change information elapsed time the calculated elapsed time is remembered to be by password table 24b is reached, while generating a new initial entry and transmitting to a client 10, the value of the initial entry already recorded on initial entry table 26b is updated to a new thing. Moreover, initial entry generation time of day is reset and updated at the time of day at that event at this time.

[0047] That is, in the gestalt of this operation, when predetermined time has passed since generation of an initial entry, while authentication and initial entry generator 20b generate a new initial entry and transmits to a client 10, it functions also as 2nd renewal means of an initial entry which memorizes the new initial entry to initial entry table 26b.

[0048] Hereafter, actuation of this communication system which has this configuration is explained based on flow drawing shown in drawing 8 and drawing 9 . Since flow drawing shown in drawing 8 adds the processing flow S300 which updates the initial entry generation time of day of initial entry table 26b between S107 and S108 in flow drawing shown in drawing 2 , it attaches the same sign as drawing 2 about other processings, and stops it to easy explanation here.

[0049] First, in flow drawing shown in drawing 8 , authentication and initial entry generator 20b receive a demand signal from a client 10 (S101), and when the initial entry is included in the demand signal, as shown in (S102) and drawing 9 , user authentication of a client 10 is performed based on the initial entry and initial entry table 26b (S301). And if the user authentication of the client 10 using an initial entry goes wrong, the communication link between a client 10 and server 12b will be ended.

[0050] On the other hand, if it succeeds in the user authentication of the client 10 using an initial entry, authentication and initial entry generator 20b will be subtracted from the current time outputted from the internal clock which does not illustrate the initial entry generation time of day memorized by initial entry table 26b next, and will derive the elapsed time t from the event of generating an initial entry to current (S302). Furthermore, authentication and the initial entry generator 20 read the connection change information elapsed time T from password table 24a (S303), and compares the value and value of the elapsed time t drawn by S302 (S304).

[0051] And if elapsed time t is a value smaller than the connection change information elapsed time T, processing will be moved to S108 (drawing 8), it will usually pass, and access processing to the server program 22 will be performed (S108). On the other hand, if elapsed time t is beyond the connection change information elapsed time T, authentication and initial entry generator 20b will generate a new initial entry (S305), will store it in initial entry table 26b, and will update an initial entry (S306). Furthermore, authentication and initial entry generator 20b are reset at the current time outputted from the internal clock which does not illustrate the value of the initial entry generation time of day of initial entry table 26b (S300, drawing 8). Then, it usually passes and access processing to the server program 22 is performed (S108). Under the present circumstances, the initial entry transmitted to a client 10 in S111 is newly generated in S305. A client program 16 receives this new initial entry from server 12b, and updates the old initial entry already memorized by the storage means 18.

[0052] According to the gestalt of this operation explained above, an initial entry is updated when fixed time amount has passed since the time of day which generated the initial entry. That is, the period which can receive user authentication by the server by the same initial entry is restricted to a fixed period. While being able to lessen by this possibility that an initial entry will be intercepted, also when an initial entry is intercepted, unlawful access which used the initial entry and which is depended for becoming completely can be restricted.

[0053] Gestalt 4. drawing 10 of operation is the functional block diagram showing the communication system concerning the gestalt 4 of operation of this invention. The communication system shown in this drawing is applied to the combination of the technique of the communication system concerning the gestalt 2 of the above-mentioned implementation, and the technique of the communication system concerning the gestalt 3 of the above-mentioned implementation, is looked like [the content of password table 24c and initial entry table 26c, and processing of authentication and initial entry generator 20c], and has the description. And since the server program 22 of a client 10 and its internal configuration, and server 12c is the same as that of the communication system concerning the gestalt 1 of operation, it attaches the same sign here and omits explanation.

[0054] First, it matches with a user name and a password and each user's count of connection change information and connection change information progress time of day are memorized by password table 24c of the communication system concerning the gestalt of this operation. The count of connection change information is the set point which determines the updating conditions of the initial entry memorized by initial entry table 26c as well as the gestalt 2 of the above-mentioned implementation, and a setting-out input is beforehand done by the user of a client 10 or server 12c with the input means which is not illustrated. Moreover, connection change information elapsed time is the set point which determines the updating conditions of the initial entry memorized by initial entry table 26c as well as the gestalt 3 of the above-mentioned implementation, and a setting-out input is beforehand done by the user of a client 10 or server 12c with the input means which is not illustrated.

[0055] Moreover, it matches with a user name and an initial entry, and each user's count of access and initial entry generation time of day are memorized by initial entry table 26c of the communication system concerning the gestalt of this operation. After an initial entry is generated and the count of access is stored in initial entry table 26c like the gestalt 2 of the above-mentioned implementation, it expresses the next count of access of the client 10. Moreover, initial entry generation time of day expresses the time of day when the initial entry was generated like the gestalt 3 of the above-mentioned implementation.

[0056] On the other hand, whenever authentication and initial entry generator 20c of this communication system have access of a client 10, it increments and updates the column of the count of access of initial entry table 26c. And if the value of the count of connection change information the count of access is remembered to be by password table 24c is reached, while generating a new initial entry and transmitting to a client 10, the value of the initial entry already recorded on initial entry table 26c is updated to a new thing. Moreover, the value of the count of access is reset to 0 at this time. Furthermore, whenever authentication and initial entry generator 20c have access of a client 10, it calculates the elapsed time from the initial entry generation time of day of initial entry table 26c. And if the value of the connection change information elapsed time the calculated elapsed time is remembered to be by password table 24c is reached, while generating a new initial entry and transmitting to a client 10, the value of the initial entry already recorded on initial entry table 26c is updated to a new thing. Moreover, initial entry generation time of day is reset and updated at the time of day at that event at this time.

[0057] Hereafter, actuation of this communication system which has this configuration is explained based on flow drawing shown in drawing 11 and drawing 12 . Since flow drawing shown in drawing 11 adds the processing flow S400 which resets the count of access of initial entry table 26c to 0 between S107 and S108 in flow drawing shown in drawing 2 , and the processing flow S401 which updates the initial entry generation time of day of initial entry table 26c, it attaches the same sign as drawing 2 about other processings, and stops it to easy explanation here.

[0058] First, in flow drawing shown in drawing 5 , authentication and initial entry generator 20c receive a demand signal from a client 10 (S101), and when the initial entry is included in the demand signal, as shown in (S102) and drawing 12 , user authentication of a client 10 is performed based on the initial entry and initial entry table 26c (S402). And if the user authentication of the client 10 using an initial entry goes wrong, the communication link between a client 10 and server 12c will be ended.

[0059] On the other hand, if it succeeds in the user authentication of the client 10 using an initial entry, authentication and initial entry generator 20c will increment the value of the count of access memorized by initial entry table 26c next, and will update the value n of the count of access of initial entry table 26c (S403). Furthermore, authentication and initial entry generator 20c read the value K of the count of connection change information from password table 24c (S404), and compares the value and value of the count of access (S405).

[0060] And if it is a value beyond the value K whose value n of the count of

access is a count of connection change information, authentication and initial entry generator 20c will generate a new initial entry (S409), will store it in initial entry table 26c, and will update an initial entry (S410). Furthermore, while authentication and initial entry generator 20c reset the value n of the count of access of initial entry table 26c to 0 (S400), it is reset at the current time outputted from the internal clock which does not illustrate the value of the initial entry generation time of day of the initial entry table 26 (S401). Then, it usually passes and access processing to the server program 22 is performed (S108). Under the present circumstances, the initial entry transmitted to a client 10 in S111 is newly generated in S409. A client program 16 receives this new initial entry from server 12b, and updates the old initial entry already memorized by the storage means 18.

[0061] On the other hand, if the value n of the count of access is judged to be a value smaller than the value K which is a count of connection change information by S405 next, authentication and initial entry generator 20c will be subtracted from the current time outputted from the internal clock which does not illustrate the initial entry generation time of day memorized by initial entry table 26c, and the elapsed time t from the event of generating an initial entry to the present will be derived (S406). Furthermore, authentication and initial entry generator 20c read the connection change information elapsed time T from password table 24c (S407), and compares the value and value of the elapsed time t drawn by S406 (S408).

[0062] And if elapsed time t is a value smaller than the connection change information elapsed time T, processing will be moved to S108, it will usually pass, and access processing to the server program 22 will be performed. On the other hand, if elapsed time t is beyond the connection change information elapsed time T, authentication and initial entry generator 20c will generate a new initial entry (S409), will store it in initial entry table 26c, and will update an initial entry (S410). And while authentication and the initial entry generator 20 reset the value n of the count of access of the initial entry table 26 to 0 (S400), it is reset at the current time outputted from the internal clock which does not illustrate the value of the initial entry generation time of day of the initial entry table 26 (S401). Then, it usually passes and access processing to the server program 22 is performed (S108).

[0063] When fixed time amount has passed since the time of day which generated the initial entry according to the gestalt of this operation explained above, or after generating an initial entry, in a certain case, the initial entry is updated for access by the same initial entry more than the count of predetermined. That is, the count and period which can receive user authentication by the server by the same initial entry are restricted to the fixed range. While being able to lessen by this possibility that an initial entry

will be intercepted, also when an initial entry is intercepted, unlawful access which used the initial entry and which is depended for becoming completely can be restricted.

[0064] In addition, only when it is the case where the count n of access is more than the count K of connection change information and elapsed time t is beyond the connection change information elapsed time T, you may make it update an initial entry in the above-mentioned explanation, although the initial entry was updated when the count n of access was more than the count K of connection change information, or also when it was any in case elapsed time t is beyond the connection change information elapsed time T.

[0065] Gestalt 5. drawing 13 of operation is the functional block diagram showing the communication system concerning the gestalt 5 of operation of this invention. As compared with the communication system concerning the gestalt of each above-mentioned implementation, the communication system shown in this drawing is looked like [the content (password table 24d and initial entry table 26d) and processing of authentication and 20d of initial entry generators], and has the description. And since the configuration of a client 10 and the server 12d server program 22 are the same as that of the communication system concerning the gestalt of each above-mentioned implementation, they attach the same sign here and omit explanation.

[0066] First, it matches with a user name and a password and each user's time-out time amount is memorized by password table 24d of the communication system concerning the gestalt of this operation. This time-out time amount is the set point which determines the conditions which delete the initial entry memorized by initial entry table 26d, and a setting-out input is beforehand done by a client 10 or the server 12d user with the input means which is not illustrated.

[0067] Moreover, it matches with a user name and an initial entry, and each user's last access time of day is memorized by initial entry table 26d of the communication system concerning the gestalt of this operation. Access time of day expresses last time the time of day when the client 10 accessed server 12d last time [this].

[0068] On the other hand, whenever authentication and 20d of initial entry generators of this communication system have access of a client 10, they calculate the elapsed time from the initial entry table 26d last access time of day. And if the value of the time-out time amount the calculated elapsed time is remembered to be by password table 24d is reached, the user's initial entry will be deleted from initial entry table 26d, and transmission of a user name and a password will be again required from a client 10. If the time-out time amount the calculated elapsed time is remembered to be by password table 24d is not reached, while generating a new initial entry and transmitting to a client 10 on the other hand, the value of the initial entry already

recorded on initial entry table 26d is updated to a new thing. Moreover, access time of day is reset and updated at the time of day at that event last time at this time.

[0069] That is, in the gestalt of this operation, even if predetermined time passes since the event of the last access of authentication and 20d of initial entry generators, when there is no access from the again same client, it functions also as 1st authentication termination means which once stops the user authentication of the client 10 by authentication and 20d (authentication means) of initial entry generators.

[0070] Hereafter, actuation of this communication system which has this configuration is explained based on flow drawing shown in drawing 14 and drawing 15 . Since flow drawing shown in drawing 14 adds the processing flow S500 which updates the initial entry table 26d last access time of day between S107 and S108 in flow drawing shown in drawing 2 , it attaches the same sign as drawing 2 about other processings, and stops it to easy explanation here.

[0071] First, in flow drawing shown in drawing 14 , authentication and 20d of initial entry generators receive a demand signal from a client 10 (S101), and when the initial entry is included in the demand signal, as shown in (S102) and drawing 15 , user authentication of a client 10 is performed based on the initial entry and initial entry table 26d (S501). And if the user authentication of the client 10 using an initial entry goes wrong, the communication link between a client 10 and server 12d will be ended.

[0072] On the other hand, if it succeeds in the user authentication of the client 10 using an initial entry, authentication and 20d of initial entry generators will be subtracted from the current time outputted from the internal clock which does not illustrate access time of day last time which is memorized by initial entry table 26d next, and they will derive the elapsed time t from the time of day when the client 10 concerned accessed the server 12 last time to current (S502). Furthermore, authentication and 20d of initial entry generators read the time-out time amount T from password table 24d (S503), and they compare the value and value of the elapsed time t drawn by S502 (S504).

[0073] And if elapsed time t is a value smaller than the time-out time amount T, authentication and 20d of initial entry generators will generate a new initial entry (S505), they will store it in initial entry table 26d, and will update an initial entry (S506). Furthermore, authentication and 20d of initial entry generators are reset at the current time outputted from the internal clock which does not illustrate the value of the initial entry table 26d last access time of day (S500). Then, it usually passes and access processing to the server program 22 is performed (S108). Under the present circumstances, the initial entry transmitted to a client 10 in S111 is newly generated in S505.

A client program 16 receives this new initial entry from server 12d, and updates the old initial entry already memorized by the storage means 18.

[0074] On the other hand, if elapsed time t is a value beyond the time-out time amount T, authentication and 20d of initial entry generators will delete the initial entry of the client 10 from initial entry table 26d (S507). Then, transmission of a user name and a password is again required from a client 10 (S103).

[0075] According to the gestalt of this operation explained above, when spacing of access from a client 10 exceeds fixed time amount, the initial entry registered at the event is deleted from initial entry table 26d. That is, if a client 10 does not carry out sequential access within fixed time amount to server 12d, it becomes invalid [an initial entry], and user authentication with a user name and a password is needed again. In this way, according to the gestalt of this operation, unlawful access which an initial entry can prevent tapping, consequently depends for becoming completely can be prevented.

[0076] Moreover, server 12d since [from a client 10] an initial entry is updated at every access, unlawful access which can lessen possibility of tapping of an initial entry and is depended for becoming completely can be prevented so that clearly [S504-S506 of drawing 15].

[0077] Gestalt 6. drawing 16 of operation is the functional block diagram showing the communication system concerning the gestalt 6 of operation of this invention. As compared with the communication system concerning the gestalt of each above-mentioned implementation, the communication system shown in this drawing is looked like [the content of password table 24e and initial entry table 26e, and processing of authentication and initial entry generator 20e], and has the description. And since the server program 22 of the configuration of a client 10 and server 12e is the same as that of the communication system concerning the gestalt of each above-mentioned implementation, it attaches the same sign here and omits explanation.

[0078] First, it matches with a user name and a password and each user's count of initial entry deletion is memorized by password table 24e of the communication system concerning the gestalt of this operation. This count of initial entry deletion is the set point which determines the conditions which delete the initial entry memorized by initial entry table 26e, and a setting-out input is beforehand done by the user of a client 10 or server 12e with the input means which is not illustrated.

[0079] Moreover, it matches with a user name and an initial entry, and each user's count of access is memorized by initial entry table 26e of the communication system concerning the gestalt of this operation like the communication system concerning an example 2. After a new initial entry is generated and this count of access is stored in initial entry table 26e, it expresses the next count of access of that client 10.

[0080] On the other hand, whenever authentication and initial entry generator 20e of this communication system have access of a client 10, it increments and updates the value of the count of access of initial entry table 26e. And if the value of the count of initial entry deletion the count of access is remembered to be by password table 24e is reached, the user's initial entry will be deleted from initial entry table 26e, and transmission of a user name and a password will be again required from a client 10. If it has not become the count of initial entry deletion the count of access is remembered to be by password table 24e, while generating a new initial entry and transmitting to a client 10 on the other hand, the value of the initial entry already recorded on initial entry table 26e is updated to a new thing.

[0081] In the gestalt of this operation, after the user authentication of the client 10 according [authentication and initial entry generator 20e] to a password, when there is access from the client more than the count of predetermined, it functions also as 2nd authentication termination means which once stops the user authentication of the client 10 by authentication and initial entry generator 20e (authentication means).

[0082] Hereafter, actuation of this communication system which has this configuration is explained based on flow drawing shown in drawing 17 and drawing 18 . Since flow drawing shown in drawing 17 adds the processing flow S600 which resets the count of access of initial entry table 26e to 0 between S107 and S108 in flow drawing shown in drawing 2 , it attaches the same sign as drawing 2 about other processings, and stops it to easy explanation here.

[0083] First, in flow drawing shown in drawing 17 , authentication and initial entry generator 20e receive a demand signal from a client 10 (S101), and when the initial entry is not included in the demand signal, user authentication of the client 10 with (S102) and a password is performed (S103-S105). Then, if it succeeds in user authentication with a password, while generating an initial entry and registering with initial entry table 26e (S106, S107), the count of access of initial entry table 26e is reset to 0 (S600).

[0084] Moreover, when the initial entry is included in the demand signal received from a client 10, as shown in (S102) and drawing 18 , user authentication of a client 10 is performed based on the initial entry and initial entry table 26e (S601). And if the user authentication of the client 10 using an initial entry goes wrong, the communication link between a client 10 and server 12e will be ended.

[0085] On the other hand, if it succeeds in the user authentication of the client 10 using an initial entry, authentication and initial entry generator 20e will increment the value of the count of access memorized by initial entry table 26e next, and will update the value n of the count of access of initial

entry table 26e (S602). Furthermore, authentication and initial entry generator 20e read the value K of the count of connection change information from password table 24e (S603), and compares the value and value of the count of access (S604). And if it is a value with the value n of the count of access smaller than the value K which is a count of connection change information, authentication and initial entry generator 20e will generate a new initial entry (S605), will store it in initial entry table 26e, and will update an initial entry (S606). Then, it usually passes and access processing to the server program 22 is performed (S108). Under the present circumstances, the initial entry transmitted to a client 10 in S111 is newly generated in S605. A client program 16 receives this new initial entry from server 12e, and updates the old initial entry already memorized by the storage means 18.

[0086] On the other hand, if it is beyond the value K whose value n of the count of access is a count of connection change information, authentication and initial entry generator 20e will delete the initial entry of the client 10 from initial entry table 26e (S607). Then, transmission of a user name and a password is again required from a client 10 (S103).

[0087] The count [e / the client 10 after performing user authentication with a password according to the gestalt of this operation explained above, and / server 12] of access counts, and if the count becomes more than the count of predetermined, user authentication with a password will be again called for from a client 10. That is, according to the gestalt of this operation, user authentication with a password is performed at every access of the count of predetermined between a client 10 and server 12e. Consequently, also when an initial entry should be revealed to other users, unlawful access can be restricted in the count of predetermined.

[0088] Gestalt 7. drawing 19 of operation is the functional block diagram showing the communication system concerning the gestalt 7 of operation of this invention. As compared with the communication system concerning the gestalt of each above-mentioned implementation, the communication system shown in this drawing is looked like [the content (password table 24f and initial entry table 26f) and processing of authentication and 20f of initial entry generators], and has the description. And since the configuration of a client 10 and the server 12f server program 22 are the same as that of the communication system concerning the gestalt of each above-mentioned implementation, they attach the same sign here and omit explanation.

[0089] First, it matches with a user name and a password and each user's initial entry deletion elapsed time is memorized by password table 24f of the communication system concerning the gestalt of this operation. This initial entry deletion elapsed time is the set point which determines the conditions which delete the initial entry memorized by initial entry table 26f, and a

setting-out input is beforehand done by a client 10 or the server 12f user with the input means which is not illustrated.

[0090] Moreover, like the communication system concerning an example 3, it matches with a user name and an initial entry, and each user's initial entry generation time of day is memorized by initial entry table 26f of the communication system concerning the gestalt of this operation. This initial entry generation time of day expresses the time of day when the initial entry was generated.

[0091] On the other hand, whenever authentication and 20f of initial entry generators of this communication system have access of a client 10, they calculate the elapsed time of initial entry table 26f initial entry generation time of day to the event of the access. And if the value of the initial entry deletion elapsed time the calculated elapsed time is remembered to be by password table 24f is reached, the user's initial entry will be deleted from initial entry table 26f, and transmission of a user name and a password will be again required from a client 10. If the initial entry deletion elapsed time the calculated elapsed time is remembered to be by password table 24f is not reached, while generating a new initial entry and transmitting to a client 10 on the other hand, the value of the initial entry already recorded on initial entry table 26f is updated to a new thing.

[0092] In the gestalt of this operation, after the user authentication of the client 10 with a password, when predetermined time passes, it functions also as 3rd authentication termination means which once stops the user authentication of the client 10 by authentication and 20f of initial entry generators.

[0093] Hereafter, actuation of this communication system which has this configuration is explained based on flow drawing shown in drawing 20 and drawing 21 . Since flow drawing shown in drawing 20 adds the processing flow S700 which updates initial entry table 26f initial entry generation time of day to current time between S107 and S108 in flow drawing shown in drawing 2 , it attaches the same sign as drawing 2 about other processings, and stops it to easy explanation here.

[0094] First, in flow drawing shown in drawing 20 , authentication and 20f of initial entry generators receive a demand signal from a client 10 (S101), and when the initial entry is not included in the demand signal, user authentication of the client 10 with (S102) and a password is performed (S103-S105). Then, if it succeeds in user authentication with a password, while generating an initial entry and registering with initial entry table 26f (S106, S107), it resets to the value of the current time outputted from the internal clock which does not illustrate the value of initial entry table 26f initial entry generation time of day (S700).

[0095] Moreover, when the initial entry is included in the demand signal

received from a client 10, as shown in (S102) and drawing 21 , user authentication of a client 10 is performed based on the initial entry and initial entry table 26f (S701). And if the user authentication of the client 10 using an initial entry goes wrong, the communication link between a client 10 and server 12f will be ended.

[0096] On the other hand, if it succeeds in the user authentication of the client 10 using an initial entry, authentication and 20f of initial entry generators will be subtracted from the current time outputted from the internal clock which does not illustrate the initial entry generation time of day memorized by initial entry table 26f next, and they will derive the elapsed time t from the event of generating an initial entry to current (S702). Furthermore, authentication and 20f of initial entry generators read the connection change information elapsed time T from password table 24f (S703), and they compare the value and value of the elapsed time t drawn by S702 (S704).

[0097] And if elapsed time t is a value smaller than the connection change information elapsed time T, authentication and 20f of initial entry generators will generate a new initial entry (S705), they will store it in initial entry table 26f, and will update an initial entry (S706). Then, it usually passes and access processing to the server program 22 is performed (S108). Under the present circumstances, the initial entry transmitted to a client 10 in S111 is newly generated in S705. A client program 16 receives this new initial entry from server 12f, and updates the old initial entry already memorized by the storage means 18.

[0098] On the other hand, if elapsed time t is beyond the connection change information elapsed time T, authentication and 20f of initial entry generators will delete the initial entry of the client 10 from initial entry table 26f (S707). Then, transmission of a user name and a password is again required from a client 10 (S103).

[0099] If fixed time amount passes after performing user authentication with a password according to the gestalt of this operation explained above, user authentication with a password will be again called for from a client 10. That is, according to the gestalt of this operation, user authentication with a password whenever it goes through predetermined time is performed. Consequently, also when an initial entry should be revealed to other users, unlawful access can be restricted in predetermined time.

[0100] Gestalt 8. drawing 22 of operation is the functional block diagram showing the communication system concerning the gestalt 8 of operation of this invention. The communication system shown in this drawing is applied to the combination of the technique of the communication system concerning the gestalt 6 of the above-mentioned implementation, and the technique of the communication system concerning the gestalt 7 of the above-mentioned

implementation, is looked like [the content (password table 24g and initial entry table 26g) and processing of authentication and 20g of initial entry generators], and has the description. And since a client 10 and its internal configuration, and the server 12g server program 22 are the same as that of the communication system concerning the gestalt 1 of operation, they attach the same sign here and omit explanation.

[0101] First, it matches with a user name and a password and each user's count of initial entry deletion and initial entry deletion elapsed time are memorized by password table 24g of the communication system concerning the gestalt of this operation. The count of initial entry deletion and initial entry deletion elapsed time are the set points which determine the conditions which delete the initial entry memorized by initial entry table 26g, and a setting-out input is beforehand done by a client 10 or the server 12g user with the input means which is not illustrated.

[0102] Moreover, it matches with a user name and an initial entry, and like the communication system concerning an example 6, while each user's count of access is memorized by initial entry table 26g of the communication system concerning the gestalt of this operation, each user's initial entry generation time of day is memorized by it like the communication system concerning an example 7. After a new initial entry is generated and the count of access is stored in initial entry table 26g, it expresses the next count of access of the client 10. Initial entry generation time of day expresses the time of day when the initial entry was generated.

[0103] On the other hand, whenever authentication and 20g of initial entry generators of this communication system have access of a client 10, they increment and update the value of the initial entry table 26g count of access. And if the value of the count of initial entry deletion the count of access is remembered to be by password table 24g is reached, the user's initial entry will be deleted from initial entry table 26g, and transmission of a user name and a password will be again required from a client 10.

[0104] moreover, even when the count of initial entry deletion the count of access is remembered to be by password table 24g is not become If the value of the initial entry deletion elapsed time with which calculate the elapsed time of initial entry table 26g initial entry generation time of day to the event of the access, and the calculated elapsed time is remembered to be by password table 24g is reached The user's initial entry is deleted from initial entry table 26g, and transmission of a user name and a password is again required from a client 10.

[0105] If the initial entry deletion elapsed time with which, on the other hand, do not become the count of initial entry deletion the count of access is remembered to be by password table 24g, and elapsed time is remembered to be by password table 24g is not reached, while generating a new initial

entry and transmitting to a client 10, the value of the initial entry already recorded on initial entry table 26g is updated to a new thing.

[0106] Hereafter, actuation of this communication system which has this configuration is explained based on flow drawing shown in drawing 23 and drawing 24 . Since flow drawing shown in drawing 23 adds the processing flow S800 which resets the initial entry table 26g count of access to 0 between S107 and S108 in flow drawing shown in drawing 2 , and the processing flow S801 which updates initial entry table 26g initial entry generation time of day at current time, it attaches the same sign as drawing 2 about other processings, and stops it to easy explanation here.

[0107] First, in flow drawing shown in drawing 23 , authentication and 20g of initial entry generators receive a demand signal from a client 10 (S101), and when the initial entry is not included in the demand signal, user authentication of the client 10 with (S102) and a password is performed (S103-S105). Then, if it succeeds in user authentication with a password, an initial entry will be generated and it will register with initial entry table 26g (S106, S107). Moreover, while resetting the initial entry table 26g count of access to 0 (S800), it resets to the value of the current time outputted from the internal clock which does not illustrate the value of the initial entry generation time of day of initial entry table 26e (S801).

[0108] Moreover, when the initial entry is included in the demand signal received from a client 10, as shown in (S102) and drawing 24 , user authentication of a client 10 is performed based on the initial entry and initial entry table 26g (S802). And if the user authentication of the client 10 using an initial entry goes wrong, the communication link between a client 10 and server 12g will be ended.

[0109] On the other hand, if it succeeds in the user authentication of the client 10 using an initial entry, authentication and 20g of initial entry generators will increment the value of the count of access memorized by initial entry table 26g next, and they will update the value n of the initial entry table 26g count of access (S803). Furthermore, authentication and 20g of initial entry generators read the value K of the count of initial entry deletion from password table 24g (S804), and they compare the value and value of the count of access (S805).

[0110] And if it is a value with the value n of the count of access smaller than the value K which is a count of initial entry deletion, authentication and 20g of initial entry generators will be subtracted from the current time outputted from the internal clock which does not illustrate the initial entry generation time of day memorized by initial entry table 26g next, and the elapsed time t from the event of generating an initial entry to the present will be derived (S806). Furthermore, authentication and 20g of initial entry generators read the initial entry deletion elapsed time T from password table

24g (S807), and they compare the value and value of the elapsed time t drawn by S806 (S808).

[0111] And if elapsed time t is a value smaller than the initial entry deletion elapsed time T, authentication and 20g of initial entry generators will generate a new initial entry (S809), they will store it in initial entry table 26g, and will update an initial entry (S810). Then, it usually passes and access processing to the server program 22 is performed (S108). Under the present circumstances, the initial entry transmitted to a client 10 in S111 is newly generated in S809. A client program 16 receives this new initial entry from server 12g, and updates the old initial entry already memorized by the storage means 18.

[0112] On the other hand, when it is beyond the value K whose value n of the count of access is a count of initial entry deletion, or when elapsed time t is beyond the initial entry deletion elapsed time T, authentication and 20g of initial entry generators delete the initial entry of the client 10 from initial entry table 26g (S811). Then, transmission of a user name and a password is again required from a client 10 (S103).

[0113] After performing user authentication with a password, when fixed time amount has passed according to the gestalt of this operation explained above, or when [after performing user authentication with a password,·] access of the count of predetermined occurs, user authentication with a password is again called for from a client 10. Consequently, also when an initial entry should be revealed to other users, unlawful access can be restricted to the inside of the count of predetermined, and predetermined time.

[0114] In addition, only when it is the case where the count n of access is more than the count K of initial entry deletion and elapsed time t is beyond the initial entry deletion elapsed time T, you may make it delete an initial entry in the above-mentioned explanation, although the initial entry was deleted when the count n of access was more than the count K of initial entry deletion, or also when it was any in case elapsed time t is beyond the initial entry deletion elapsed time T.

[0115] The communication system concerning the gestalt 9 of operation of gestalt 9. this invention of operation is the same configuration as the communication system concerning the gestalt 1 of the above-mentioned implementation, and a part of actuation of authentication and the initial entry generator 20 merely differs. Specifically, processing which replaces the communication system concerning the gestalt of this operation with the processing which authentication and the initial entry generator 20 show in flow drawing of drawing 3 in drawing 2 which shows actuation of the communication system concerning the gestalt 1 of operation, and flow drawing of drawing 3 , and is shown in flow drawing of drawing 25 is

performed. Thereby, in the communication system concerning the gestalt of this operation, the user of a client 10 can cancel himself the initial entry published to self compulsorily.

[0116] That is, in the gestalt of this operation, when the predetermined demand signal of a purport with which the authentication initial entry generator 20 should cancel an initial entry from a client 10 is received, it functions also as 4th authentication termination means which stops the user authentication of the client 10 by authentication and initial entry program 20d (authentication means).

[0117] Hereafter, actuation of this communication system which has this configuration is explained based on flow drawing shown in drawing 2 and drawing 25 .

[0118] First, in flow drawing shown in drawing 2 , authentication and the initial entry generator 20 receive a demand signal from a client 10 (S101), and when the initial entry is included in the demand signal, as shown in (S102) and drawing 25 , user authentication of a client 10 is performed based on the initial entry and initial entry table 26 (S901). And if the user authentication of the client 10 using an initial entry goes wrong, the communication link between a client 10 and a server 12 will be ended.

[0119] On the other hand, if it succeeds in the user authentication of the client 10 using an initial entry, authentication and the initial entry generator 20 will judge whether the initial entry deletion demand is included in the demand signal received from the client 10 (S902). And if contained, the user's initial entry will be deleted from the initial entry table 26 (S903), and the communication link between a client 10 and a server 12 will be ended. On the other hand, if the initial entry deletion demand is not included in the demand signal received from the client 10, it usually passes and access processing to the server program 22 is performed (S108).

[0120] According to the gestalt of this operation explained above, a user can cancel an initial entry, when an initial entry can be compulsorily cancelled of its volition, consequently a user judges that it is itself unnecessary, and he can prevent unlawful access depended for becoming completely.

[0121] Gestalt 10. drawing 26 of operation is the functional block diagram showing the communication system concerning the gestalt 10 of operation of this invention. The communication system shown in this drawing has the description at the point that the client 10 is equipped with the automatic access program 28, as compared with the communication system concerning the gestalt of each above-mentioned implementation. This automatic access program 28 is an executive program (applet) which a client program 16 receives from authentication and the initial entry generator 20, and carries out automatic access for every fixed time amount by controlling the communication facility of a client program 16 at a server 12. In addition,

since the configuration of a client program 16 and a server is the same as that of the communication system concerning the gestalt of each above-mentioned implementation, it attaches the same sign here and omits explanation.

[0122] In the gestalt of this operation, the automatic access program 28, and the authentication and the initial entry generator 20 which transmit this automatic access program 28 to a client 10 function as a client-server access generating means to generate access to a server 12 from the client 10 for every fixed time amount using an initial entry.

[0123] Hereafter, actuation of this communication system which has this configuration is explained based on flow drawing shown in drawing 27 and drawing 28 . Since flow drawing shown in drawing 27 adds the processing flow S112 which transmits the automatic access program 28 after S111 at a client 10 in flow drawing shown in drawing 2 , it attaches the same sign as drawing 2 about other processings, and stops it to easy explanation here.

[0124] As shown in drawing 27 , if the initial entry is not included in the demand signal received from the client 10, by the server 12, authentication and the initial entry generator 20 require a user name and a password from a client 10 first (S103). On the other hand, if a user name and a password are received from a client 10 (S104), authentication and the initial entry generator 20 will perform user authentication of a client 10 based on the user name and password which were received, and password table 24 next. If authentication and the initial entry generator 20 succeed in the user authentication of the client 10 on the password table 24 (S105), an initial entry will be generated (S106) and additional record of the initial entry will be carried out with a user name at the initial entry table 26 (S107). Next, authentication and the initial entry generator 20 transmit the demand signal for acquiring server information while transmitting User Information, such as a user name, to the server program 22 (S108) (S109). And authentication and the initial entry generator 20 transmit the server information received from the server program 22 to a client 10 while transmitting the initial entry generated by S106 to a client 10 (S110) (S111). If the client program 16 has not yet received the automatic access program 28 when server information is received, it requires transmission of the automatic access program 28 from a server 12. On the other hand, a server 12 transmits the demanded automatic access program 28 to a client 10 (S112). For example, in a WWW system, a client program 16 acquires the applet which is the automatic access program 28 from a server 12 according to the tag information, when the tag information on the purport which should acquire an applet from a server 12 is included in the hypertext which is server information.

[0125] By controlling the communication facility of a client program 16, this automatic access program 28 accesses a server 12 for every fixed time amount, and transmits the initial entry stored in the memory of a client 10 with the demand signal of the purport which requires server information to a server 12 in that case.

[0126] In a server 12, if the demand signal accompanied by the initial entry from this automatic access program 28 is received, authentication and the initial entry generator 20 will perform user authentication of the client 10 using the initial entry table 26 (S1001). And if the user authentication of a client 10 goes wrong, the communication link between a client 10 and a server 12 will be ended. On the other hand, if it succeeds in the user authentication of the client 10 on the initial entry table 26, authentication and the initial entry generator 20 will generate a new initial entry (S1002), and will make the initial entry table 26 carry out the overwrite storage of the new initial entry that the initial entry should be updated (S1003).

[0127] According to the gestalt of this operation explained above, access between a client 10 and a server 12 occurs in a fixed time interval by the automatic access program 28. And while being able to lessen possibility of tapping of an initial entry by updating an initial entry, for example at every access, also when an initial entry should be revealed, unlawful access by the initial entry can be controlled.

[0128] In addition, various deformation implementation is possible for the communication system explained above. For example, if access is from a client 10 after passing beyond fixed time amount since access time of day last time by combining the technique of the communication system concerning the gestalt 5 of operation, the initial entry of the client 10 can be deleted from the initial entry table 26, and a user name and a password can also be again required of a user. Moreover, as long as it passes beyond fixed time amount since the last access time of day, you may make it delete the user's initial entry automatically from the initial entry table 26. Anyway, if it passes beyond fixed time amount since the last access time of day and will be made to perform user authentication with a user name and a password to the user again, unlawful access of spoofing etc. can be prevented still more certainly.

[0129] Moreover, although the communication system explained above transmitted the automatic access program 28 to the client 10 from the server 12 In a WWW system, to for example, the hypertext (server information) which transmits to a client 10 from a server 12 The tag information on the purport which should acquire the same hypertext again after predetermined time is included, and this tag information is interpreted by the client 10, and you may make it, acquire again the same hypertext as the hypertext which received immediately before from a server 12 after predetermined time on the other hand. even if it carries out like this, access with a client 10 and a server 12 is generated for every predetermined time

JP,11-167551,A [DETAILED DESCRIPTION] http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje

-- it can make -- becoming completely -- etc. -- unlawful access can be prevented.

[0130] Gestalt 11. drawing 29 of operation is the functional block diagram showing the communication system concerning the gestalt 11 of operation of this invention. As compared with the communication system which the communication system shown in this drawing requires for the gestalt 10 of the above-mentioned implementation, a client 10 is equipped with a client program 16 and client program 16a, and the automatic access program 28 has the description at the point which carries out automatic access at a server 12 using the communication facility of client program 16a. And since other configurations are the same as that of the communication system concerning the gestalt of each above-mentioned implementation, they attach the same sign here and omit explanation.

[0131] Drawing 30 and drawing 28 are flow drawings explaining actuation of the communication system concerning the gestalt of this operation. Here, flow drawing shown in drawing 30 adds the processing flow S113 which transmits the starting instruction of client program 16a to a client 10 while transmitting the automatic access program 28 after S111 at a client 10 in flow drawing shown in drawing 27 , and it attaches the same sign as drawing 27 about other processings. Moreover, in S102, if it judges that the initial entry is not included in the demand signal which authentication and the initial entry generator 20 received from the client 10, this authentication and initial entry generator 20 will shift processing to already shown flow drawing of drawing 28 .

[0132] As shown in these drawings, authentication and the initial entry generator 20 of a server 12 When it succeeds in the user authentication of the client 10 on the password table 24 (S105), Or when it succeeds in the user authentication of the client 10 on the initial entry table 26 (S1001), Server information with a demand is transmitted to a client 10 (S111), and the automatic access program 28 and the starting instruction of client program 16a are transmitted to a client 10 in that case (S113). Then, in a client 10, if these automatic access program 28 and the starting instruction of client program 16a are received, while a client program 16 will start client program 16a, the received automatic access program 28 is performed as a child process of the client program 16a. And the automatic access program 28 transmits the demand signal of the purport which requires the same server information as the server information which the client program 16 has received immediately before using the communication facility which client program 16a has to a server 12 after predetermined time.

[0133] In a server 12, if the demand signal accompanied by the initial entry from this automatic access program 28 is received, authentication and the initial entry generator 20 will perform user authentication of the client 10 using the initial entry table 26 (S1001). And if the user authentication of a client 10 goes wrong, the communication link between a client 10 and a server 12 will be ended. On the other hand, if it succeeds in the user authentication of the client 10 on the initial entry table 26, authentication and the initial entry generator 20 will generate a new initial entry (S1002), and will make the initial entry table 26 carry out the overwrite storage of the new initial entry that the initial entry should be updated (S1003).

[0134] According to the gestalt of this operation explained above, it can prevent the client program which can divide the client program which a user operates actually, and the client program which the automatic access program 28 uses for automatic access, consequently a user operates by automatic access locking. Therefore, when a user, for example, wants to transmit the new demand signal of the purport which requires other server information to a server 12 according to the gestalt of this operation, the situation where the automatic access program 28 is using the client program 16, and cannot transmit promptly can be avoided.

[0135] Gestalt 12. drawing 31 of operation is the functional block diagram showing the communication system concerning the gestalt 12 of operation of this invention. The communication system shown in this drawing has the description as compared with the communication system concerning the gestalt 1 of operation at the point that the client 10 is equipped with the code program 30, and the point of having the function in which authentication and 20h of initial entry generators decode encryption by this code program 30. Here, in case the code program 30 transmits a user name and a password to a server 12, it is a program which enciphers them. That is, in the gestalt of this operation, when the password with which authentication and 20h of initial entry generators were enciphered from the client 10 is transmitted, it functions also as a decryption means to decrypt this password. Since other configurations are the same as that of the communication system concerning the gestalt 1 of operation, they attach the same sign here and omit explanation.

[0136] Drawing 32 and drawing 3 are flow drawings explaining actuation of the communication system concerning the gestalt of this operation. Flow drawing shown in drawing 32 here establishes the processing flow S1200 which receives the user name and password which replaced with S104 in flow drawing shown in drawing 2 , and were enciphered by the code program 30, adds further the processing flow S1201 which decodes the user name and password, and attaches the same sign as drawing 2 about other processings. Moreover, in S102, if it judges that the initial entry is not included in the demand signal which authentication and 20h of initial entry generators of a server 12 received from the client 10, authentication and 20h of these initial entry generators will shift processing to already shown flow

drawing of drawing 3 .
[0137] In these drawings, if the initial entry is not included in the demand signal received from a client 10, authentication and 20h of initial entry generators of a server 12 transmit the signal which requires a user name and a password from a client 10 (S103). On the other hand, in a client 10, a client program 16 enciphers a user name and a password using the code program 30. And a client program 16 transmits the user name and password which were enciphered to a server 12.
[0138] If the user name and password which were enciphered are received (S1200), authentication and 20h of initial entry generators of a server 12 will perform decryption processing to these information, and they will acquire a user name and a password (S1201). And user authentication of a client 10 is performed using these information and password tables 24 (S105).
[0139] Since the user name and password which are used as authentication information on a first stage can be enciphered, transmitted and received according to the gestalt of this operation explained above, leakage of a password can be prevented still more certainly.
[0140] In addition, various deformation implementation is possible for the communication system concerning the gestalt of this operation explained above. For example, although the user name of a client 10 and the both sides of a password were enciphered by the code program 30 in the above-mentioned explanation, you may decide to encipher only a password.
[0141]
[Effect of the Invention] When it succeeds in user authentication with a password, in order to make user authentication by the initial entry after that according to this invention, the opportunity for a password to be sent out on a network can be decreased and the possibility of unlawful access by password leakage can be decreased.
[0142] Moreover, since according to this invention the initial entry was updated when the same initial entry was received more than the count of predetermined from a client, or when predetermined time had passed since generation of an initial entry, also when an initial entry is intercepted, the opportunity of unlawful access which used the initial entry can be taken.
[0143] Moreover, even if predetermined time passes since the event of access of 1 last time, when there is no access from the again same client according to this invention, 2) When there is access after user authentication with a password from the client more than the count of predetermined, or when predetermined time passes, 3) Since the initial entry [finishing / generation] was cancelled when the predetermined demand signal of the purport which should cancel an initial entry from a client was received While being able to lessen possibility that an initial entry will be intercepted, also when an initial entry is intercepted, the opportunity of unlawful access which used the initial entry can be taken.
[0144] Moreover, since it was made to generate access to a server from the client using an initial entry for every fixed time amount, it cannot wait for access by the user, but ** can also make an initial entry update according to this invention. Thereby, possibility of leakage of an initial entry can be lessened. Under the present circumstances, according to this invention, since it was made to access between [every] the up Norikazu scheduled time from the client using an initial entry to a server in another process with the process of a body slack client, actuation of the process of a body slack client is securable.
[0145] Furthermore, since it can be enciphered, sent and received on the occasion of transmission of the password from a client to a server according to this invention, leakage of a password can be prevented.

[Translation done.]

TECHNICAL FIELD

[Field of the Invention] Especially this invention relates to the access-control technique over the client of a server about the access-control approach of a server and a server, and an information record medium.

[Translation done.]

PRIOR ART

[Description of the Prior Art] In the connectionless environment where the client is answered, communication link connection is not maintained between client-server in the server information to which a server corresponds to the demand signal from a client. Therefore, if a client program tends to acquire the information on the server by which the access control is carried out, even if it is the case where it has already succeeded in user authentication, the authentication by the input of a user name or a password whenever a client transmits a demand signal to a server is needed. For this reason, when a demand signal was transmitted to a server, the user had to enter the user name and the password in the client, had to transmit them to the server, and had the problem that actuation became complicated.
[0003] On the other hand, once it memorizes the user name and the password in the memory on the machine of a client and succeeds in user authentication with a user name and a password in access to a certain server, by access to the same subsequent server, avoiding this problem will also be considered by transmitting the user name and password on memory automatically each time.

[Translation done.]

* NOTICES *

JPO and NCIPI are not responsible for any damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

EFFECT OF THE INVENTION

[Effect of the Invention] When it succeeds in user authentication with a password, in order to make user authentication by the initial entry after that according to this invention, the opportunity for a password to be sent out on a network can be decreased and the possibility of unlawful access by password leakage can be decreased.
[0142] Moreover, since according to this invention the initial entry was updated when the same initial entry was received more than the count of predetermined from a client, or when predetermined time had passed since generation of an initial entry, also when an initial entry is intercepted, the opportunity of unlawful access which used the initial entry can be taken.
[0143] Moreover, even if predetermined time passes since the event of access of 1 last time, when there is no access from the again same client according to this invention, 2) When there is access after user authentication with a password from the client more than the count of predetermined, or when predetermined time passes, 3) Since the initial entry [finishing / generation] was cancelled when the predetermined demand signal of the purport which should cancel an initial entry from a client was received While being able to lessen possibility that an initial entry will be intercepted, also when an initial entry is intercepted, the opportunity of unlawful access which used the initial entry can be taken.
[0144] Moreover, since it was made to generate access to a server from the client using an initial entry for every fixed time amount, it cannot wait for access by the user, but ** can also make an initial entry update according to this invention. Thereby, possibility of leakage of an initial entry can be lessened. Under the present circumstances, according to this invention, since it was made to access between [every] the up Norikazu scheduled time from the client using an initial entry to a server in another process with the process of a body slack client, actuation of the process of a body slack client is securable.

JP,11-167551,A [EFFECT OF THE INVENTION] http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje

[0145] Furthermore, since it can be enciphered, sent and received on the occasion of transmission of the password from a client to a server according to this invention, leakage of a password can be prevented.

[Translation done.]

TECHNICAL PROBLEM

[Problem(s) to be Solved by the Invention] However, in the access control between client-server, authentication information, such as a user name and a password, being transmitted by simple text data in many cases, and transmitting a password at every access to a server from a client as mentioned above has the problem of being easy to cause unlawful access to the increase of the danger of tapping, and a user depended for becoming completely.

[0005] On the other hand, in the security method concerning JP,4-182768,A, secret enquiry information is changed at every access in the communication environment which establishes a connection. That is, in this method, user authentication of a client is performed by using the password information of immobilization, and the secret enquiry information which changes each time by the pair for connection establishment with a host computer. However, since transmission and reception of a password are frequently performed between a client and a host computer also in this technique, the danger of tapping of such information is high. Since secret enquiry information is furthermore saved at a client, there is a problem that a host computer can be accessed only from the client.

[0006] This invention is made in view of the above-mentioned technical problem, and the object is in offering the information record medium which recorded the program which realizes the access-control approach of a server and a server and it which can lessen possibility of leakage of authentication information in the access control between client-server.

[Translation done.]

* NOTICES *

JPO and NCIPI are not responsible for any damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

MEANS

[Means for Solving the Problem] In the server which answers the client in the server information corresponding to the demand signal with which the 1st invention is transmitted from a client in order to solve the above-mentioned technical problem An initial entry transmitting means to generate an initial entry to the client which succeeded in user authentication with a password, and to transmit to it, A connection information storage means to memorize the initial entry transmitted to a client with said initial entry transmitting means, An authentication means to perform user authentication of a client based on the initial entry and the initial entry memorized by said connection information storage means when the initial entry matched with the demand signal from the client is received, When it succeeds in the user authentication of a client with said authentication means, a server information reply means to answer a client in the server information corresponding to the demand signal matched with the initial entry is included.

[0008] In the 1st invention, the 2nd invention includes further the 1st renewal means of an initial entry which memorizes the new initial entry for said connection information storage means while it generates a new initial entry and transmits to a client, when the same initial entry is received more than the count of predetermined from a client.
[0009] In the 1st or 2nd invention, the 3rd invention includes further the 2nd renewal means of an initial entry which memorizes the new initial entry for said connection information storage means while it generates a new initial entry and transmits to a client, when predetermined time has passed since generation of the initial entry by said initial entry transmitting means.
[0010] In the 1st thru/or the 3rd one of invention, the 4th invention includes further the 1st authentication termination means which once stops the user authentication of the client by said authentication means, when there is no access from the again same client, even if predetermined time passes since

the event of the last access.
[0011] In the 1st thru/or the 4th one of invention, after the user authentication of a client with a password, the 5th invention includes further the 2nd authentication termination means which once stops the user authentication of the client by said authentication means, when there is access from the client more than the count of predetermined.
[0012] In the 1st thru/or the 5th one of invention, after the user authentication of a client with a password, the 6th invention includes further the 3rd authentication termination means which once stops the user authentication of the client by said authentication means, when predetermined time passes.
[0013] In the 1st thru/or the 6th one of invention, the 7th invention includes further the 4th authentication termination means which stops the user authentication of the client by said authentication means, when the predetermined demand signal of the purport which should cancel an initial entry from a client is received.
[0014] The 8th invention includes further a client-server access generating means to generate access to a server from the client for every fixed time amount using an initial entry, in the 1st thru/or the 7th one of invention.
[0015] In the 8th invention, the 9th invention includes an activation module transmitting means to transmit the activation module which controls a client so that said client-server access generating means may perform access to the server using an initial entry for every fixed time amount to a client.
[0016] In the 8th invention, said server information of the 10th invention is hypertext information, and said client-server access generating means includes the tag information on a purport that access to the server which used the initial entry should be performed after predetermined time in said server information.
[0017] In the 1st thru/or the 9th one of invention, the 11th invention is further equipped with a decryption means to decrypt this password, when the password enciphered from the client is transmitted.
[0018] The 12th invention the server information corresponding to the demand signal transmitted from a client The initial entry transmitting step which is the access-control approach of the server which answers the client, generates an initial entry to the client which succeeded in user authentication with a password, and is transmitted to it, The connection information storage step which memorizes the initial entry transmitted to a client at said initial entry transmitting step, The authentication step which performs user authentication of a client based on the initial entry and the initial entry memorized at said connection information storage step when the initial entry matched with the demand signal from the client is received, When it succeeds in the user authentication of a client at said authentication step,

the server information reply step which answers a client in the server information corresponding to the demand signal matched with the initial entry is included.

[0019] The 13th invention the server information corresponding to the demand signal to which a computer is transmitted from a client The initial entry transmitting step which is the information record medium which recorded the program for making it operate as a server which answers the client, generates an initial entry to the client which succeeded in user authentication with a password, and is transmitted to it, The connection information storage step which memorizes the initial entry transmitted to a client at said initial entry transmitting step, The authentication step which performs user authentication of a client based on the initial entry and the initial entry memorized at said connection information storage step when the initial entry matched with the demand signal from the client is received, When it succeeds in the user authentication of a client at said authentication step, the program for making a computer perform the server information reply step which answers a client in the server information corresponding to the demand signal matched with the initial entry is recorded.

[0020]

[Embodiment of the Invention] Hereafter, the gestalt of operation of this invention is explained to a detail based on a drawing.

[0021] Gestalt 1. drawing 1 of operation is the functional block diagram showing the communication system concerning the gestalt 1 of operation of this invention. Below, it clarifies about one of the operation gestalten of the information record medium which recorded the program for realizing the access-control approach of the server concerning this invention, a client, and a server, and it through disclosure of this communication system.

[0022] As shown in this drawing, a client 10 and a server 12 are mutually connected by the means of communications 14, such as the Internet, possible [a communication link], and this communication system becomes. And in this communication system, communication link connection of a client 10 and the server 12 is made in the connectionless environment, and a client 10 transmits the demand signal of the purport which requires server information from a server 12. On the other hand, a server 12 answers the client 10 in the server information corresponding to the demand signal received from a client 10. This configuration is common in a WWW (World Wide Web) system etc., the above-mentioned demand signal is equivalent to URL (Uniform Resource Locator) in this case, and the above-mentioned server information is equivalent to hypertext information.

[0023] A client 10 is constituted by information processors, such as PC, and contains the client program 16 which is loaded to main storage and performed by CPU. And the initial entry is especially memorized by the

storage means 18, such as memory. If server information is received from a server 12 to the demand signal while this client program 16 transmits a demand signal to a server 12 through means of communications 14, it will perform the display display based on the server information with the indicating equipment which is not illustrated. Moreover, a client program 16 transmits the initial entry to a server 12 with a demand signal, when the initial entry is memorized by the storage means 18.

[0024] The server 12 includes the authentication and the initial entry generator 20 which is constituted by information processors, such as PC, is loaded to main storage like a client 10, and is performed by CPU, and the server program 22. And the password table 24 and the initial entry table 26 are memorized by especially the external storage.

[0025] First, authentication and the initial entry generator 20 perform user authentication of a client 10 based on the information and password table 24, when a user name and a password are transmitted from a client program 16. And when it succeeds in the user authentication of a client 10, while generating the initial entry over the client 10 and transmitting to a client 10, this information is matched with a user name and it memorizes on the initial entry table 26.

[0026] Moreover, authentication and the initial entry generator 20 perform user authentication of a client 10 based on the initial entry and initial entry table 26, when an initial entry is transmitted with a demand signal from a client program 16. And when it succeeds in the user authentication of a client 10, transmission of the server information which a client 10 requires from the server program 22 is required of the server program 22, and the server information received from the server program 22 is transmitted to a client 10.

[0027] Here, the server program 22 is a program which answers a letter in server information, when a demand signal is received. Moreover, the user name (ID) of the user who is planning that a server 12 is accessed, and the password and ** which were given to the user are matched with the password table 24, and it memorizes. Furthermore, the initial entry table 26 is a table on which the initial entry generated by authentication and the initial entry generator 20 is memorized, and the initial entry and ** which were generated to the user name and user name of the client 10 which accessed the server 12 are matched, and it is memorized.

[0028] In addition, in the server 12 contained in the above communication system, authentication and the initial entry generator 20 function as an initial entry transmitting means to generate an initial entry to the client 10 which succeeded in user authentication with a password, and to transmit to it. Moreover, the initial entry table 26 functions as a connection information storage means to memorize the initial entry transmitted to a client 10 with

an initial entry transmitting means. Furthermore, authentication and the initial entry generator 20 When the initial entry matched with the demand signal from the client 10 is received, while functioning as an authentication means to perform user authentication of a client 10, based on the initial entry and the initial entry memorized by the connection information storage means When it succeeds in the user authentication of a client 10 with an authentication means, it functions as a server information reply means to transmit the server information corresponding to the demand signal matched with the initial entry to a client 10.

[0029] Hereafter, actuation of this communication system which has this configuration is explained based on flow drawing shown in drawing 2 and drawing 3 .

[0030] As shown in drawing 2 , by the server 12, authentication and the initial entry generator 20 receive the demand signal from a client 10 first (S101). And it judges whether the initial entry is included in the received demand signal (S102), and if the initial entry is not included, a user name and a password are required from a client 10 (S103). On the other hand, if a user name and a password are received from a client 10 (S104), authentication and the initial entry generator 20 will perform user authentication of a client 10 based on the user name and password which were received, and password table 24 next. And if the user authentication of the client 10 on the password table 24 goes wrong (S105), the communications processing between a client 10 and a server 12 will be ended.

[0031] Moreover, if authentication and the initial entry generator 20 succeed in the user authentication of the client 10 on the password table 24 in S105, an initial entry will be generated (S106) and additional record of the initial entry will be carried out with a user name at the initial entry table 26 (S107). This initial entry is enciphered and generated by the random combination of a figure, a notation, and an alphabetic character. Next, authentication and the initial entry generator 20 transmit the demand signal for acquiring server information while transmitting User Information, such as a user name, to the server program 22 (S108) (S109). User Information transmitted to the server program 22 can be used if required of the server program 22 concerned. And authentication and the initial entry generator 20 transmit the server information received from the server program 22 to a client 10 while transmitting the initial entry generated by S106 to a client 10 (S110) (S111).

[0032] When it is judged that the initial entry is included in the demand signal which authentication and the initial entry generator 20 receive from a client 10 in S102 on the other hand, user authentication of a client 10 is performed by investigating whether next the initial entry of this authentication and initial entry generator 20 is the same as that of what is already recorded on the initial entry table 26 (S112). And if it succeeds in the user authentication of a client 10 (S113), processing will be moved to S108 and processing for answering a letter in server information to a client 10 will be performed. Moreover, if the user authentication of a client 10 goes wrong in S113, the communication link between a client 10 and a server 12 will be ended.

[0033] Since the count to which an exchange of a password is performed between a client 10 and a server 12 can be lessened according to the gestalt of the operation explained above, unlawful access by leakage of a password can be prevented. Moreover, if an initial entry can be changed frequently, it can be made to function as a dynamic password so to speak and it carries out like this, leakage of the initial entry situation can also be prevented and unlawful access can be prevented still more certainly.

[0034] Gestalt 2. drawing 4 of operation is the functional block diagram showing the communication system concerning the gestalt 2 of operation of this invention. The communication system shown in this drawing is looked like [the content of password table 24a and initial entry table 26a, and processing of authentication and initial entry generator 20a], and has the description. And since the server program 22 of a client 10 and its internal configuration, and server 12a is the same as that of the communication system concerning the gestalt 1 of operation, it attaches the same sign here and omits explanation.

[0035] First, it matches with a user name and a password and each user's count of connection change information is memorized by password table 24a of the communication system concerning the gestalt of this operation. This count of connection change information is the set point which determines the updating conditions of the initial entry memorized by initial entry table 26a, and a setting-out input is beforehand done by the user of a client 10 or a server 12 with the input means which is not illustrated.

[0036] Moreover, it matches with a user name and an initial entry, and each user's count of access is memorized by initial entry table 26a of the communication system concerning the gestalt of this operation. After an initial entry is generated and this count of access is stored in initial entry table 26a, it expresses the next count of access of that client 10.

[0037] On the other hand, whenever authentication and initial entry generator 20a of this communication system have access of a client 10, it increments and updates the column of the count of access of the initial entry table 26. And if the value of the count of connection change information the count of access is remembered to be by password table 24a is reached, while generating a new initial entry and transmitting to a client 10, the value of the initial entry already recorded on initial entry table 26a is updated to a new thing. Moreover, the value of the count of access is reset to 0 at this time.

[0038] That is, in the gestalt of this operation, when authentication and initial

entry generator 20a receive the same initial entry more than the count of predetermined from a client, while generating a new initial entry and transmitting to a client 10, it functions also as 1st renewal means of an initial entry which memorizes the new initial entry to initial entry table 26a.

[0039] Hereafter, actuation of this communication system which has this configuration is explained based on flow drawing shown in drawing 5 and drawing 6 . Since flow drawing shown in drawing 5 adds the processing flow S200 which resets the count of access of initial entry table 26a to 0 between S107 and S108 in flow drawing shown in drawing 2 , it attaches the same sign as drawing 2 about other processings, and stops it to easy explanation here.

[0040] First, in flow drawing shown in drawing 5 , authentication and initial entry generator 20a receive a demand signal from a client 10 (S101), and when the initial entry is included in the demand signal, as shown in (S102) and drawing 6 , user authentication of a client 10 is performed based on the initial entry and initial entry table 26 (S201). And if the user authentication of the client 10 using an initial entry goes wrong, the communication link between a client 10 and a server 12 will be ended.

[0041] On the other hand, if it succeeds in the user authentication of the client 10 using an initial entry, authentication and the initial entry generator 20 will increment the value of the count of access memorized by initial entry table 26a next, and will update the value n of the count of access of initial entry table 26a (S202). Furthermore, authentication and the initial entry generator 20 read the value K of the count of connection change information from password table 24a (S203), and compares the value and value of the count of access (S204). And if it is a value with the value n of the count of access smaller than the value K which is a count of connection change information, processing will be moved to S108 (drawing 5), it will usually pass, and access processing to the server program 22 will be performed (S108). On the other hand, if it is beyond the value K whose value n of the count of access is a count of connection change information, authentication and the initial entry generator 20 will generate a new initial entry (S205), will store it in the initial entry table 26, and will update an initial entry (S206). Furthermore, authentication and the initial entry generator 20 reset the value n of the count of access of the initial entry table 26 to 0 (S200, drawing 5). Then, it usually passes and access processing to the server program 22 is performed (S108). Under the present circumstances, the initial entry transmitted to a client 10 in S110 is newly generated in S205. A client program 16 receives this new initial entry from a server 12, and updates the old initial entry already memorized by the storage means 18.

[0042] According to the gestalt of the operation explained above, an initial entry is updated when the count of access becomes more than the count of fixed. While being able to lessen by this possibility that an initial entry will be intercepted, also when an initial entry is intercepted, unlawful access which used the initial entry and which is depended for becoming completely can be restricted.

[0043] Gestalt 3. drawing 7 of operation is the functional block diagram showing the communication system concerning the gestalt 3 of operation of this invention. As compared with the communication system concerning the gestalt 1 of operation, or 2, the communication system shown in this drawing is looked like [the content of password table 24b and initial entry table 26b, and processing of authentication and initial entry generator 20b], and has the description. And since the server program 22 of the configuration of a client 10 and server 12b is the same as that of the communication system concerning the gestalt 1 of operation, or 2, it attaches the same sign here and omits explanation.

[0044] First, it matches with a user name and a password and each user's connection change information elapsed time is memorized by password table 24b of the communication system concerning the gestalt of this operation. This connection change information elapsed time is the set point which determines the updating conditions of the initial entry memorized by initial entry table 26b, and a setting-out input is beforehand done by the user of a client 10 or server 12b with the input means which is not illustrated.

[0045] Moreover, it matches with a user name and an initial entry, and each user's initial entry generation time of day is memorized by initial entry table 26b of the communication system concerning the gestalt of this operation. This initial entry generation time of day expresses the time of day when the initial entry was generated.

[0046] On the other hand, whenever authentication and initial entry generator 20b of this communication system have access of a client 10, it calculates the elapsed time from the initial entry generation time of day of initial entry table 26b. And if the value of the connection change information elapsed time the calculated elapsed time is remembered to be by password table 24b is reached, while generating a new initial entry and transmitting to a client 10, the value of the initial entry already recorded on initial entry table 26b is updated to a new thing. Moreover, initial entry generation time of day is reset and updated at the time of day at that event at this time.

[0047] That is, in the gestalt of this operation, when predetermined time has passed since generation of an initial entry, while authentication and initial entry generator 20b generate a new initial entry and transmits to a client 10, it functions also as 2nd renewal means of an initial entry which memorizes the new initial entry to initial entry table 26b.

[0048] Hereafter, actuation of this communication system which has this configuration is explained based on flow drawing shown in drawing 8 and drawing 9 . Since flow drawing shown in drawing 8 adds the processing flow

JP,11-167551,A [MEANS] http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje

S300 which updates the initial entry generation time of day of initial entry table 26b between S107 and S108 in flow drawing shown in drawing 2 , it attaches the same sign as drawing 2 about other processings, and stops it to easy explanation here.

[0049] First, in flow drawing shown in drawing 8 , authentication and initial entry generator 20b receive a demand signal from a client 10 (S101), and when the initial entry is included in the demand signal, as shown in (S102) and drawing 9 , user authentication of a client 10 is performed based on the initial entry and initial entry table 26b (S301). And if the user authentication of the client 10 using an initial entry goes wrong, the communication link between a client 10 and server 12b will be ended.

[0050] On the other hand, if it succeeds in the user authentication of the client 10 using an initial entry, authentication and initial entry generator 20b will be subtracted from the current time outputted from the internal clock which does not illustrate the initial entry generation time of day memorized by initial entry table 26b next, and will derive the elapsed time t from the event of generating an initial entry to current (S302). Furthermore, authentication and the initial entry generator 20 read the connection change information elapsed time T from password table 24a (S303), and compares the value and value of the elapsed time t drawn by S302 (S304).

[0051] And if elapsed time t is a value smaller than the connection change information elapsed time T, processing will be moved to S108 (drawing 8), it will usually pass, and access processing to the server program 22 will be performed (S108). On the other hand, if elapsed time t is beyond the connection change information elapsed time T, authentication and initial entry generator 20b will generate a new initial entry (S305), will store it in initial entry table 26b, and will update an initial entry (S306). Furthermore, authentication and initial entry generator 20b are reset at the current time outputted from the internal clock which does not illustrate the value of the initial entry generation time of day of initial entry table 26b (S300, drawing 8). Then, it usually passes and access processing to the server program 22 is performed (S108). Under the present circumstances, the initial entry transmitted to a client 10 in S111 is newly generated in S305. A client program 16 receives this new initial entry from server 12b, and updates the old initial entry already memorized by the storage means 18.

[0052] According to the gestalt of this operation explained above, an initial entry is updated when fixed time amount has passed since the time of day which generated the initial entry. That is, the period which can receive user authentication by the server by the same initial entry is restricted to a fixed period. While being able to lessen by this possibility that an initial entry will be intercepted, also when an initial entry is intercepted, unlawful access which used the initial entry and which is depended for becoming completely can be restricted.

[0053] Gestalt 4. drawing 10 of operation is the functional block diagram showing the communication system concerning the gestalt 4 of operation of this invention. The communication system shown in this drawing is applied to the combination of the technique of the communication system concerning the gestalt 2 of the above-mentioned implementation, and the technique of the communication system concerning the gestalt 3 of the above-mentioned implementation, is looked like [the content of password table 24c and initial entry table 26c, and processing of authentication and initial entry generator 20c], and has the description. And since the server program 22 of a client 10 and its internal configuration, and server 12c is the same as that of the communication system concerning the gestalt 1 of operation, it attaches the same sign here and omits explanation.

[0054] First, it matches with a user name and a password and each user's count of connection change information and connection change information progress time of day are memorized by password table 24c of the communication system concerning the gestalt of this operation. The count of connection change information is the set point which determines the updating conditions of the initial entry memorized by initial entry table 26c as well as the gestalt 2 of the above-mentioned implementation, and a setting-out input is beforehand done by the user of a client 10 or server 12c with the input means which is not illustrated. Moreover, connection change information elapsed time is the set point which determines the updating conditions of the initial entry memorized by initial entry table 26c as well as the gestalt 3 of the above-mentioned implementation, and a setting-out input is beforehand done by the user of a client 10 or server 12c with the input means which is not illustrated.

[0055] Moreover, it matches with a user name and an initial entry, and each user's count of access and initial entry generation time of day are memorized by initial entry table 26c of the communication system concerning the gestalt of this operation. After an initial entry is generated and the count of access is stored in initial entry table 26c like the gestalt 2 of the above-mentioned implementation, it expresses the next count of access of the client 10. Moreover, initial entry generation time of day expresses the time of day when the initial entry was generated like the gestalt 3 of the above-mentioned implementation.

[0056] On the other hand, whenever authentication and initial entry generator 20c of this communication system have access of a client 10, it increments and updates the column of the count of access of initial entry table 26c. And if the value of the count of connection change information the count of access is remembered to be by password table 24c is reached, while generating a new initial entry and transmitting to a client 10, the value

of the initial entry already recorded on initial entry table 26c is updated to a new thing. Moreover, the value of the count of access is reset to 0 at this time. Furthermore, whenever authentication and initial entry generator 20c have access of a client 10, it calculates the elapsed time from the initial entry generation time of day of initial entry table 26c. And if the value of the connection change information elapsed time the calculated elapsed time is remembered to be by password table 24c is reached, while generating a new initial entry and transmitting to a client 10, the value of the initial entry already recorded on initial entry table 26c is updated to a new thing. Moreover, initial entry generation time of day is reset and updated at the time of day at that event at this time.

[0057] Hereafter, actuation of this communication system which has this configuration is explained based on flow drawing shown in drawing 11 and drawing 12 . Since flow drawing shown in drawing 11 adds the processing flow S400 which resets the count of access of initial entry table 26c to 0 between S107 and S108 in flow drawing shown in drawing 2 , and the processing flow S401 which updates the initial entry generation time of day of initial entry table 26c, it attaches the same sign as drawing 2 about other processings, and stops it to easy explanation here.

[0058] First, in flow drawing shown in drawing 5 , authentication and initial entry generator 20c receive a demand signal from a client 10 (S101), and when the initial entry is included in the demand signal, as shown in (S102) and drawing 12 , user authentication of a client 10 is performed based on the initial entry and initial entry table 26c (S402). And if the user authentication of the client 10 using an initial entry goes wrong, the communication link between a client 10 and server 12c will be ended.

[0059] On the other hand, if it succeeds in the user authentication of the client 10 using an initial entry, authentication and initial entry generator 20c will increment the value of the count of access memorized by initial entry table 26c next, and will update the value n of the count of access of initial entry table 26c (S403). Furthermore, authentication and initial entry generator 20c read the value K of the count of connection change information from password table 24c (S404), and compares the value and value of the count of access (S405).

[0060] And if it is a value beyond the value K whose value n of the count of access is a count of connection change information, authentication and initial entry generator 20c will generate a new initial entry (S409), will store it in initial entry table 26c, and will update an initial entry (S410). Furthermore, while authentication and initial entry generator 20c reset the value n of the count of access of initial entry table 26c to 0 (S400), it is reset at the current time outputted from the internal clock which does not illustrate the value of the initial entry generation time of day of the initial entry table 26 (S401). Then, it usually passes and access processing to the server program 22 is performed (S108). Under the present circumstances, the initial entry transmitted to a client 10 in S111 is newly generated in S409. A client program 16 receives this new initial entry from server 12b, and updates the old initial entry already memorized by the storage means 18.

[0061] On the other hand, if the value n of the count of access is judged to be a value smaller than the value K which is a count of connection change information by S405 next, authentication and initial entry generator 20c will be subtracted from the current time outputted from the internal clock which does not illustrate the initial entry generation time of day memorized by initial entry table 26c, and the elapsed time t from the event of generating an initial entry to the present will be derived (S406). Furthermore, authentication and initial entry generator 20c read the connection change information elapsed time T from password table 24c (S407), and compares the value and value of the elapsed time t drawn by S406 (S408).

[0062] And if elapsed time t is a value smaller than the connection change information elapsed time T, processing will be moved to S108, it will usually pass, and access processing to the server program 22 will be performed. On the other hand, if elapsed time t is beyond the connection change information elapsed time T, authentication and initial entry generator 20c will generate a new initial entry (S409), will store it in initial entry table 26c, and will update an initial entry (S410). And while authentication and the initial entry generator 20 reset the value n of the count of access of the initial entry table 26 to 0 (S400), it is reset at the current time outputted from the internal clock which does not illustrate the value of the initial entry generation time of day of the initial entry table 26 (S401). Then, it usually passes and access processing to the server program 22 is performed (S108).

[0063] When fixed time amount has passed since the time of day which generated the initial entry according to the gestalt of this operation explained above, or after generating an initial entry, in a certain case, the initial entry is updated for access by the same initial entry more than the count of predetermined. That is, the count and period which can receive user authentication by the server by the same initial entry are restricted to the fixed range. While being able to lessen by this possibility that an initial entry will be intercepted, also when an initial entry is intercepted, unlawful access which used the initial entry and which is depended for becoming completely can be restricted.

[0064] In addition, only when it is the case where the count n of access is more than the count K of connection change information and elapsed time t is beyond the connection change information elapsed time T, you may make it update an initial entry in the above-mentioned explanation, although the

initial entry was updated when the count n of access was more than the count K of connection change information, or also when it was any in case elapsed time t is beyond the connection change information elapsed time T.

[0065] Gestalt 5. drawing 13 of operation is the functional block diagram showing the communication system concerning the gestalt 5 of operation of this invention. As compared with the communication system concerning the gestalt of each above-mentioned implementation, the communication system shown in this drawing is looked like [the content (password table 24d and initial entry table 26d) and processing of authentication and 20d of initial entry generators], and has the description. And since the configuration of a client 10 and the server 12d server program 22 are the same as that of the communication system concerning the gestalt of each above-mentioned implementation, they attach the same sign here and omit explanation.

[0066] First, it matches with a user name and a password and each user's time-out time amount is memorized by password table 24d of the communication system concerning the gestalt of this operation. This time-out time amount is the set point which determines the conditions which delete the initial entry memorized by initial entry table 26d, and a setting-out input is beforehand done by a client 10 or the server 12d user with the input means which is not illustrated.

[0067] Moreover, it matches with a user name and an initial entry, and each user's last access time of day is memorized by initial entry table 26d of the communication system concerning the gestalt of this operation. Access time of day expresses last time the time of day when the client 10 accessed server 12d last time [this].

[0068] On the other hand, whenever authentication and 20d of initial entry generators of this communication system have access of a client 10, they calculate the elapsed time from the initial entry table 26d last access time of day. And if the value of the time-out time amount the calculated elapsed time is remembered to be by password table 24d is reached, the user's initial entry will be deleted from initial entry table 26d, and transmission of a user name and a password will be again required from a client 10. If the time-out time amount the calculated elapsed time is remembered to be by password table 24d is not reached, while generating a new initial entry and transmitting to a client 10 on the other hand, the value of the initial entry already recorded on initial entry table 26d is updated to a new thing. Moreover, access time of day is reset and updated at the time of day at that event last time at this time.

[0069] That is, even if predetermined time passes since the event of the last access of authentication and 20d of initial entry generators, when there is no access from the again same client in the gestalt of this operation, they are authentication and 20d of initial entry generators.

[Translation done.]

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] It is the functional block diagram showing the communication system concerning the gestalt 1 of operation of this invention.
[Drawing 2] It is flow drawing explaining actuation of the communication system concerning the gestalt 1 of operation of this invention.
[Drawing 3] It is flow drawing explaining actuation of the communication system concerning the gestalt 1 of operation of this invention.
[Drawing 4] It is the functional block diagram showing the communication system concerning the gestalt 2 of operation of this invention.
[Drawing 5] It is flow drawing explaining actuation of the communication system concerning the gestalt 2 of operation of this invention.
[Drawing 6] It is flow drawing explaining actuation of the communication system concerning the gestalt 2 of operation of this invention.
[Drawing 7] It is the functional block diagram showing the communication system concerning the gestalt 3 of operation of this invention.
[Drawing 8] It is flow drawing explaining actuation of the communication system concerning the gestalt 3 of operation of this invention.
[Drawing 9] It is flow drawing explaining actuation of the communication system concerning the gestalt 3 of operation of this invention.
[Drawing 10] It is the functional block diagram showing the communication system concerning the gestalt 4 of operation of this invention.
[Drawing 11] It is flow drawing explaining actuation of the communication system concerning the gestalt 4 of operation of this invention.
[Drawing 12] It is flow drawing explaining actuation of the communication system concerning the gestalt 4 of operation of this invention.
[Drawing 13] It is the functional block diagram showing the communication system concerning the gestalt 5 of operation of this invention.
[Drawing 14] It is flow drawing explaining actuation of the communication system concerning the gestalt 5 of operation of this invention.

[Drawing 15] It is flow drawing explaining actuation of the communication system concerning the gestalt 5 of operation of this invention.
[Drawing 16] It is the functional block diagram showing the communication system concerning the gestalt 6 of operation of this invention.
[Drawing 17] It is flow drawing explaining actuation of the communication system concerning the gestalt 6 of operation of this invention.
[Drawing 18] It is flow drawing explaining actuation of the communication system concerning the gestalt 6 of operation of this invention.
[Drawing 19] It is the functional block diagram showing the communication system concerning the gestalt 7 of operation of this invention.
[Drawing 20] It is flow drawing explaining actuation of the communication system concerning the gestalt 7 of operation of this invention.
[Drawing 21] It is flow drawing explaining actuation of the communication system concerning the gestalt 7 of operation of this invention.
[Drawing 22] It is the functional block diagram showing the communication system concerning the gestalt 8 of operation of this invention.
[Drawing 23] It is flow drawing explaining actuation of the communication system concerning the gestalt 8 of operation of this invention.
[Drawing 24] It is flow drawing explaining actuation of the communication system concerning the gestalt 8 of operation of this invention.
[Drawing 25] It is flow drawing explaining actuation of the communication system concerning the gestalt 9 of operation of this invention.
[Drawing 26] It is the functional block diagram showing the communication system concerning the gestalt 10 of operation of this invention.
[Drawing 27] It is flow drawing explaining actuation of the communication system concerning the gestalt 10 of operation of this invention.
[Drawing 28] It is flow drawing explaining actuation of the communication system concerning the gestalt 10 of operation of this invention.
[Drawing 29] It is the functional block diagram showing the communication system concerning the gestalt 11 of operation of this invention.
[Drawing 30] It is flow drawing explaining actuation of the communication system concerning the gestalt 11 of operation of this invention.
[Drawing 31] It is the functional block diagram showing the communication system concerning the gestalt 12 of operation of this invention.
[Drawing 32] It is flow drawing explaining actuation of the communication system concerning the gestalt 12 of operation of this invention.
[Description of Notations]
10 Client, 12, 12a-12g A server, 14 16 Means of communications, 16a A client program, 18 Storage means, 20, and 20a-20h authentication and an initial entry generator, 22 A server program, 24, 24a-24g Password table, 26, 26a-26g An initial entry table, 28 An automatic access program, 30 Code program.

[Translation done.]